

UNIVERSIDAD CARLOS III DE MADRID

TRABAJO FIN DE GRADO



**INTEROPERABILIDAD ENTRE SENSORES
DE HUELLA PLANAR Y DE HUELLA
RODADA**

GRADO EN INGENIERÍA TELEMÁTICA

Autor: Laura Díaz Urbano

Tutor: Raúl Sánchez Reíllo

Co-Tutor: Belén Fernández Saavedra

Leganés, 18 de febrero de 2014

Resumen

En la actualidad, la biometría está empezando a ser muy utilizada para la identificación de personas en diversas aplicaciones. Como consecuencia existe un aumento del número de dispositivos biométricos existentes en el mercado. Asimismo, el incremento de este tipo de aplicaciones lleva a soluciones en las que los usuarios sean reclutados de forma segura una única vez, y se identifiquen para el uso de las diferentes aplicaciones.

Teniendo en cuenta estas tendencias, en este TFG se ha llevado a cabo un estudio sobre el rendimiento de algunos dispositivos, concretamente de huella dactilar, cuando el reclutamiento se ha realizado con un tipo de sensor y la verificación se realiza con un tipo distinto. El objetivo es analizar la evolución del rendimiento biométrico para estos casos en los que es necesaria la interoperabilidad de los sistemas.

En particular, para este trabajo se han escogido dispositivos diferentes de huella dactilar (diferente modelo) en los que además la forma de capturar la huella y la imagen obtenida es distinta. Es decir con uno se captura lo que se denomina huella planar o posada, y en el otro se captura la llamada huella rodada. Mediante el uso de estos sensores, se ha obtenido una base de datos (BBDD) de huellas dactilares reclutando usuarios que han acudido voluntariamente para facilitar sus datos.

Considerando esta BBDD, el trabajo realizado ha consistido en el desarrollo de dos aplicaciones. La primera de ellas ha sido creada para analizar las huellas recogidas por los distintos dispositivos con la finalidad de obtener los valores de similitud resultado de comparar unas huellas con otras.

Posteriormente, se ha desarrollado una segunda aplicación que permite calcular las tasas de error para los diferentes casos en función de los valores de similitud obtenidos previamente.

Finalmente, ambas aplicaciones han sido utilizadas en diferentes pruebas necesarias para poder llevar a cabo el estudio de interoperabilidad. Dichas pruebas permiten comparar los resultados de rendimiento de los dispositivos cuando se ha llevado a cabo el reclutamiento y la verificación con el mismo sensor con los resultados de rendimiento cuando se han empleado distintos sensores para el reclutamiento y la verificación.

El presente documento detalla todo el trabajo realizado, así como los resultados obtenidos y las conclusiones más relevantes.

Abstract

Currently, biometrics is becoming widely used for the identification of people in various applications. As a result, there is an increase of the number of biometric devices on the market. Also, the increase of these applications leads solutions that allow users to be recruited safely once, and identified for the use of different applications.

Given these trends, the TFG has conducted a study on the performance of some devices, namely fingerprint, when recruitment was made with a type of sensor and verification is performed with a different type. The objective is to analyze the evolution of biometric performance for these cases where the interoperability of systems is necessary.

In particular for this work, different fingerprint devices (different model) have been chosen. In these devices, how to capture the fingerprint and the image obtained is different. They capture planar or inn footprint and rolled fingerprint. By using these sensors, we have obtained a fingerprint database (DB) recruiting users who have come to provide their data.

Considering this DB, the work consisted in developing two applications. The first application has been developed to analyze traces collected by different devices in order to obtain the similarity values resulting from comparison with other footprints.

Subsequently, a second application has been developed to calculate the error rates for different cases based on the comparison scores.

Finally, these applications have been used in different tests to make the study of interoperability. These tests allow us to compare the results of device performance when recruitment and verification have been made with the same sensor with performance results when various sensors have been used for recruitment and verification.

This document details the work done and the results and major conclusions.

Índice

RESUMEN	1
ABSTRACT	2
ÍNDICE	3
ÍNDICE DE FIGURAS.....	5
ÍNDICE DE TABLAS.....	6
LISTADO DE ACRÓNIMOS.....	7
1 INTRODUCCIÓN	9
1.1 MOTIVACIÓN Y OBJETIVOS	9
1.2 ENTORNO SOCIO-ECONÓMICO Y MARCO REGULADOR	10
1.3 ESTRUCTURA DEL DOCUMENTO	11
2 BIOMETRÍA	12
2.1 INTRODUCCIÓN A LA BIOMETRÍA	12
2.2 MODALIDADES	12
2.2.1 ADN.....	13
2.2.2 Firma manuscrita	14
2.2.3 Voz	15
2.2.4 Rostro.....	15
2.2.5 Geometría de la mano	15
2.2.6 Dinámica de teclado	15
2.2.7 Iris	15
2.2.8 Retina.....	16
2.2.9 Huella dactilar.....	16
2.3 FUNCIONES DE UN SISTEMA BIOMÉTRICO.....	17
2.4 EVALUACIÓN DE LOS SISTEMAS BIOMÉTRICOS	18
2.4.1 Evaluación de rendimiento	18
2.4.2 Interoperabilidad	21
3 DISEÑO	23
3.1 DISEÑO DE LA APLICACIÓN.....	23
3.1.1 Requisitos generales	23
3.1.2 Requisitos específicos.....	23
3.2 HERRAMIENTAS NECESARIAS.....	25
3.2.2 Base de datos.....	25
3.2.3 Herramientas de software	35
3.2.4 Algoritmos del NIST.....	35
4 DESARROLLO	36
4.1 OBTENCIÓN DE MINUCIAS Y VALORES DE COMPARACIÓN	36
4.2 OBTENCIÓN DE TASAS DE RENDIMIENTO.....	43
5 PRUEBAS	47
5.1 PRUEBA 1	47
5.1.1 Resultados Experimento 1	49
5.1.2 Resultados Experimento 2	50



5.1.3	Resultados Prueba 1	51
5.1.4	Conclusiones Prueba 1	53
5.2	PRUEBA 2	53
5.2.1	Resultados Experimento 1	54
5.2.2	Resultados Experimento 2	55
5.2.3	Resultados Prueba 2	56
5.2.4	Conclusiones Prueba 2	58
5.3	COMPARACIÓN PRUEBA 1 CON PRUEBA 2	58
6	CONCLUSIONES Y LÍNEAS FUTURAS	60
6.1	CONCLUSIONES	60
6.2	LÍNEAS FUTURAS	60
	BIBLIOGRAFÍA	62
	ANEXO A: PLANIFICACIÓN	64
	ANEXO B: PRESUPUESTO	65
	COSTES MATERIALES	65
	COSTES DE PERSONAL	65
	COSTES TOTALES	66

Índice de Figuras

ILUSTRACIÓN 1. TIPOS DE SISTEMAS BIOMÉTRICOS	13
ILUSTRACIÓN 2. DISPOSITIVO LECTOR DE ADN	14
ILUSTRACIÓN 3. CAPTURA DE APLICACIÓN DE FIRMA MANUSCRITA	15
ILUSTRACIÓN 4. MUESTRAS DE IRIS	16
ILUSTRACIÓN 5. MUESTRAS DE HUELLA DACTILAR	17
ILUSTRACIÓN 6. FASES DEL SISTEMA BIOMÉTRICO	18
ILUSTRACIÓN 7. CURVA ROC	20
ILUSTRACIÓN 8. CURVA DET	20
ILUSTRACIÓN 9. CURVAS FNMR VS FMR	21
ILUSTRACIÓN 10. SENSOR SUPREMA BIO MINI	25
ILUSTRACIÓN 11. SENSOR SECUGEN HAMSTER IV	26
ILUSTRACIÓN 12. SENSOR SUPREMA REALSCAN-D	26
ILUSTRACIÓN 13. SENSOR UPEK EIKON FINGERPRINT READER.....	27
ILUSTRACIÓN 14. PANTALLA PRINCIPAL DE LA APLICACIÓN DE HUELLA	28
ILUSTRACIÓN 15. PANTALLA PARA RECOPIACIÓN DE DATOS PERSONALES	29
ILUSTRACIÓN 16. ERROR DE FTE	30
ILUSTRACIÓN 17. ERROR DE “TIMEOUT”	31
ILUSTRACIÓN 18. PANTALLA DE RECLUTAMIENTO	31
ILUSTRACIÓN 19. PANTALLA QUE COMPARA DOS MUESTRAS TOMADAS.....	32
ILUSTRACIÓN 20. PANTALLA DE ELECCIÓN DE VISITA	32
ILUSTRACIÓN 21. PANTALLA DE ERROR FTA	33
ILUSTRACIÓN 22. PANTALLA DE RECONOCIMIENTO	33
ILUSTRACIÓN 23. PANTALLA DE LA APLICACIÓN DE VALORES DE COMPARACIÓN	36
ILUSTRACIÓN 24. PANTALLA CON LA OPCIÓN FORMATO NIST	37
ILUSTRACIÓN 25. PANTALLA INTRODUCIENDO RUTAS PARA EXTRACCIÓN DE MINUCIAS	38
ILUSTRACIÓN 26. PANTALLA INTRODUCIENDO RUTA DE SALIDA DE VALORES DE SIMILITUD	39
ILUSTRACIÓN 27. PANTALLA INTRODUCIENDO LOS USUARIOS MÍNIMO Y MÁXIMO.....	40
ILUSTRACIÓN 28. PANTALLA DE ELECCIÓN DE DISPOSITIVO DE RECLUTAMIENTO	41
ILUSTRACIÓN 29. PANTALLA DE ELECCIÓN DE VISITAS Y DISPOSITIVO DE VERIFICACIÓN.....	42
ILUSTRACIÓN 30. CAPTURA DE PANTALLA DE LA APLICACIÓN PARA TASAS DE RENDIMIENTO	43
ILUSTRACIÓN 31. EJEMPLO GRÁFICA FAR VS FRR	44
ILUSTRACIÓN 32. EJEMPLO CURVA ROC.....	45
ILUSTRACIÓN 33. EJEMPLO CURVA DET	46
ILUSTRACIÓN 34. ESQUEMA PRUEBA 1	48
ILUSTRACIÓN 35. GRÁFICA FAR VS FRR EXPERIMENTO 1 PRUEBA 1	49
ILUSTRACIÓN 36. GRÁFICA FAR VS FRR EXPERIMENTO 2 PRUEBA 1	50
ILUSTRACIÓN 37. CURVA ROC PRUEBA 1	51
ILUSTRACIÓN 38. CURVA DET PRUEBA 1	52
ILUSTRACIÓN 39. ESQUEMA PRUEBA 2	53
ILUSTRACIÓN 40. GRÁFICA FAR VS FRR EXPERIMENTO 1 PRUEBA 2	54
ILUSTRACIÓN 41. GRÁFICA FAR VS FRR EXPERIMENTO 2 PRUEBA 2	55
ILUSTRACIÓN 42. CURVA ROC PRUEBA 2	56
ILUSTRACIÓN 43. CURVA DET PRUEBA 2	57



Índice de Tablas

TABLA 1. EJEMPLOS DE HUELLAS	27
TABLA 2. EJEMPLOS DE ERRORES	30
TABLA 3. RESUMEN DE LOS RESULTADOS	58
TABLA 4. COSTES DE PERSONAL.....	65
TABLA 5. COSTES TOTALES	66

Listado de Acrónimos

ISO	International Organization for Standardization (Organización Internacional de Normalización)
IEC	International Electrotechnical Commission (Comisión Electrotécnica Internacional)
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector (Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones)
API	Application Programming Interface (Interfaz de programación de aplicaciones)
GUTI	Grupo Universitario de Tecnologías de Identificación
TFG	Trabajo Fin de Grado
RFID	Radio Frequency Identification (Identificación por Radio Frecuencia)
ADN	Ácido desoxirribonucleico
FTE	Failure To Enrol (Fallo de reclutamiento)
FTA	Failure To Acquire (Fallo de adquisición)
FNMR	False Non-Match Rate (Tasa de falsa no coincidencia)
FMR	False Match Rate (Tasa de falsa coincidencia)
FRR	False Reject Rate (Tasa de falso rechazo)
FAR	False Accept Rate (Tasa de falsa aceptación)
GFRR	Generalized False Reject Rate (Tasa de falso rechazo general)
GFAR	Generalized False Accept Rate (Tasa de falsa aceptación general)
FNIR	False Negative Identification Rate (Tasa de falsa identificación negativa)
FPIR	False Positive Identification Rate (Tasa de falsa identificación positiva)
EER	Equal Error Rate (Tasa de igual error)
ROC	Receiver Operating Characteristic (Característica de funcionamiento del receptor)



- DET** Detection Error Trade-off (Curva de compensación por error)
- NIST** National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología)
- BBDD** Base de Datos

1 Introducción

En este documento se va a describir la tarea realizada durante el Trabajo de Fin de Grado. Este trabajo analiza las posibles diferencias en el rendimiento de los sistemas de identificación mediante huella dactilar cuando utilizan lectores de huella basados en diferentes tecnologías o diversos sistemas de adquisición. Actualmente, estos dispositivos son capaces de ayudar a la sociedad en la identificación de personas gracias a sus ventajas respecto a otras de las técnicas más empleadas, como son el uso de tokens de identificación (ej. tarjetas de crédito) o las contraseñas.

Este trabajo se ha desarrollado dentro del grupo de investigación GUTI, perteneciente a la Universidad Carlos III de Madrid, dedicado al estudio y la evaluación de los sistemas de identificación de personas.

A continuación se va a explicar la motivación y los objetivos de este trabajo, luego el entorno socio económico y posteriormente el contenido del presente documento.

1.1 Motivación y objetivos

La identificación de personas juega un papel muy importante en la actualidad. El individuo necesita identificarse para llevar a cabo diversas acciones, como realizar pagos, acceder a lugares de acceso restringido, etc. Por ello, para evitar la suplantación de la identidad y conseguir que la identificación sea más sencilla, los dispositivos biométricos pueden ser de gran utilidad.

Sin embargo, cabe destacar que en cada entidad se puede disponer de un sistema biométrico distinto, cuyo dispositivo de captura de la muestra sea diferente, ya sea por pertenecer a diferentes fabricantes o porque sus características generales son distintas. Esto supone algunos problemas a la hora de llevar a cabo una comparación entre los datos obtenidos en un lugar, con los datos del registro de la misma persona en otro lugar con otro dispositivo.

Por ello, la finalidad fundamental del presente Trabajo de Fin de Grado ha sido la realización de un estudio sobre distintos sensores de huella dactilar, concretamente de huella planar y rodada, para conocer su funcionamiento y características, y así poder obtener su interoperabilidad, es decir, el rendimiento de los sistemas biométricos en situaciones en las que el reclutamiento se ha producido con un tipo de sensor y durante la comparación se utilice un tipo diferente.

Para la consecución de dicho estudio, se ha seguido el procedimiento estándar establecido para la evaluación del rendimiento biométrico, es decir, la norma ISO/IEC 19795. Este procedimiento requiere que el algoritmo biométrico sometido a estudio procese datos reales de usuarios y se obtengan resultados de identificación. Posteriormente estos resultados deberán ser analizados y se obtendrán una serie de medidas de rendimiento que son las que permiten comparar el funcionamiento de los sistemas.

Es por ello, que el objetivo principal ha sido dividido en objetivos secundarios:

- El desarrollo de una aplicación capaz de obtener comparar muestras empleando una base de datos de la cual se pueden escoger los usuarios, las visitas y los sistemas biométricos que se quieran emplear en cada caso.
- El desarrollo de una aplicación que permita obtener las medidas de rendimiento para cada uno de los casos que se van a analizar.
- La comparación de las medidas de rendimiento para poder medir su interoperabilidad.

1.2 Entorno socio-económico y marco regulador

Como se ha mencionado en el apartado anterior, la biometría permite utilizar técnicas más seguras para la identificación de personas. Con ellas se puede evitar muchas situaciones de suplantación de identidad. Por ejemplo, mediante el empleo de tarjetas se pueden dar problemas de seguridad debido a robos de las mismas. Otra técnica muy extendida actualmente es el uso de contraseñas para redes sociales, compras por Internet, etc. En estos casos, es muy común la suplantación debido al robo de los códigos empleados. Sin embargo, la biometría permite que la identificación no dependa de factores como los citados anteriormente, si no que depende de características fisiológicas que no pueden ser suplantadas tan fácilmente.

Además de la incrementación de la seguridad frente a suplantaciones de identidad, las técnicas biométricas son una gran innovación tecnológica. La mayor parte de la gente aún no las conoce a fondo, pero promete ser una mejora de importancia para la sociedad, facilitando muchas acciones y permitiendo ahorrar mucho tiempo.

Sin embargo, también hay que mencionar que el coste que supone el uso de estos sistemas es muy elevado, debido a los materiales que se emplean y a los estudios que se deben llevar a cabo, razón que además hace más difícil su expansión. Asimismo, hay que destacar que debido al poco conocimiento existente en la sociedad sobre estas técnicas, es muy elevada la inseguridad de los individuos al facilitar sus características biométricas, como por ejemplo huella o iris, por miedo a la suplantación o pérdida de su identidad y a que no se respete su privacidad.

Por ello, para evitar los problemas de seguridad y privacidad que conlleva el uso de este tipo de sistemas, se han establecido una serie de normas por organismos como la ISO, la IEC o el UIT-T [1]. Dichas normas afectan al uso y la evaluación de los dispositivos biométricos de manera que se mejore su rendimiento a la hora de identificar a un individuo correctamente, así como definen parámetros que permitan la interoperabilidad entre los diferentes sistemas.

En concreto las normas que afectan y que se van a utilizar para el desarrollo de este TFG han sido las desarrolladas por el subcomité de normalización ISO/IEC JTC1 SC37 dedicado al campo de la biometría. Dentro de estas normas cabe destacar las normas de evaluación del rendimiento de los sistemas biométricos, es decir, la serie ISO/IEC 19795 [2], para garantizar la seguridad en la utilización de dispositivos biométricos.

Por otro lado y debido a que para llevar a cabo una evaluación de rendimiento es necesaria la adquisición de datos de los usuarios, otra de las normas que van a afectar a este TFG es la

Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, que indica cómo se deben utilizar estos datos para respetar los derechos de los individuos. [3]

1.3 Estructura del documento

Para poder explicar el trabajo realizado en el TFG, este documento ha sido dividido en diferentes apartados los cuáles se detallan a continuación.

Primero, se hablará de la biometría, donde se podrá comprender el concepto, sus fases y cómo realizar la evaluación del rendimiento y de interoperabilidad. En el siguiente capítulo se explicarán los elementos empleados para la realización de este TFG. El más importante de todos ellos ha sido la recopilación de una base de datos con muestras reales. Es por ello que este capítulo detallará el proceso seguido para la recogida de huellas dactilares describiendo cómo se ha llevado a cabo el reclutamiento de usuarios y la adquisición de sus huellas dactilares. Más adelante, se mostrarán los requisitos de diseño de las aplicaciones. Posteriormente, se explicará cómo se ha llevado a cabo el desarrollo dichas aplicaciones. Después se realizará un estudio que permitirá comparar resultados de distintas pruebas para obtener el rendimiento en interoperabilidad. Por último, se llevarán a cabo las conclusiones y líneas futuras.

Adicionalmente, se adjuntarán unos anexos con la planificación y los costes del TFG.

2 Biometría

2.1 Introducción a la biometría

El término “Biometría” se refiere a la ciencia que estudia las características y datos biológicos. Puede emplearse para conocer el comportamiento de sectores de población, influencia en enfermedades, expansión de insectos, etc.

Más concretamente, la identificación biométrica consiste en métodos de identificación de sujetos, ya sean personas, animales o cosas, mediante datos biológicos. Los parámetros pueden ser físicos, de comportamiento o ambos.

A continuación se va a explicar más en profundidad esta ciencia y la tecnología desarrollada en base a ella. En primer lugar se describirán los diferentes maneras mediante las cuales se puede llegar a identificar a una persona, es decir, las modalidades biométricas que existen. Después se describirán de forma genérica los sistemas biométricos, que son los sistemas que han sido implementados para llevar a cabo el reconocimiento de las personas. En concreto se explicarán las funciones de este tipo de sistemas. Por último se mencionará brevemente en qué consiste la evaluación de estos sistemas biométricos y los modos más habituales de realizar tal evaluación.

2.2 Modalidades

La biometría puede ayudar a la identificación de los individuos mediante parámetros físicos o de comportamiento. Estos parámetros son conocidos como características biométricas. El ser humano posee muchas de estas características, pero las que mejor se ajustan para el uso de sistemas biométricos cumplen con las propiedades de universalidad, unicidad, estabilidad, facilidad de captura, robustez frente al fraude, aceptación por parte de los usuarios y bajo coste. A continuación se explican estas características.

- La universalidad es el porcentaje de la población de la que se pueden tomar muestras.
- La unicidad se refiere a la probabilidad de que muestras de distintos individuos puedan tener las mismas características.
- La estabilidad consiste en que las características no se vean alteradas.
- La facilidad de captura trata sobre si existen sistemas con los que se puedan tomar muestras que se puedan emplear de manera sencilla.
- La robustez frente al fraude permite saber si el sujeto está siendo obligado o algún caso similar.
- La aceptación por parte de los usuarios puede depender de la comodidad, cansancio, miedo u otros factores.

Entre todas las características que se pueden utilizar, las que cumplen en mayor o menor medida las propiedades anteriores son el ADN, la firma manuscrita, la huella dactilar, la voz,

el rostro, la geometría de la mano, la dinámica del teclado, el iris o la retina. En la Ilustración 1 se pueden observar las técnicas que utilizan características fisiológicas y las que emplean características de comportamiento.

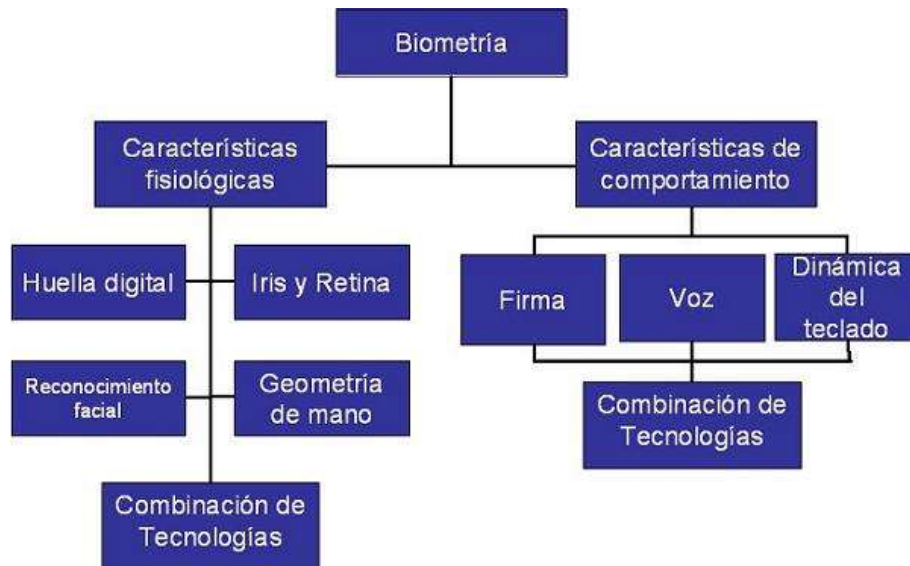


Ilustración 1. Tipos de sistemas biométricos [4]

En los siguientes apartados se van a describir algunas de las más importantes.

2.2.1 ADN

El ADN es una modalidad biométrica en la que se analizan muestras orgánicas procedentes del sujeto. Es una técnica muy fiable, pero los usuarios muestran rechazo hacia esta modalidad. Además, supone un alto coste tanto tomar las muestras como analizarlas.

En la ilustración 2 se puede ver un ejemplo de dispositivo lector de ADN.



Ilustración 2. Dispositivo lector de ADN [5]

2.2.2 Firma manuscrita

Este tipo de reconocimiento biométrico consiste en recoger una muestra de una firma realizada en la pantalla de un dispositivo y compararla con las ya existentes en la base de datos para encontrar la que más se parezca. Dentro de esta técnica, se puede decir que existen a su vez dos modalidades:

- Dinámica (on-line): se usa la información sobre cómo se ha realizado la firma, como por ejemplo la velocidad, para poder comparar también el comportamiento del usuario.
- Estática (off-line): sólo se usa el resultado final de la firma como una imagen.

Además, la aplicación busca que las dos firmas tengan ciertas características iguales para poder considerar que proceden del mismo usuario.

Como ventajas cabe destacar su facilidad de uso y aceptación por parte de los usuarios. En contra, se debe nombrar la baja unicidad, poca estabilidad de la firma y la posibilidad de fraude.

En la ilustración 3 se puede observar una captura de una aplicación que compara una firma existente en la base de datos con una muestra tomada.

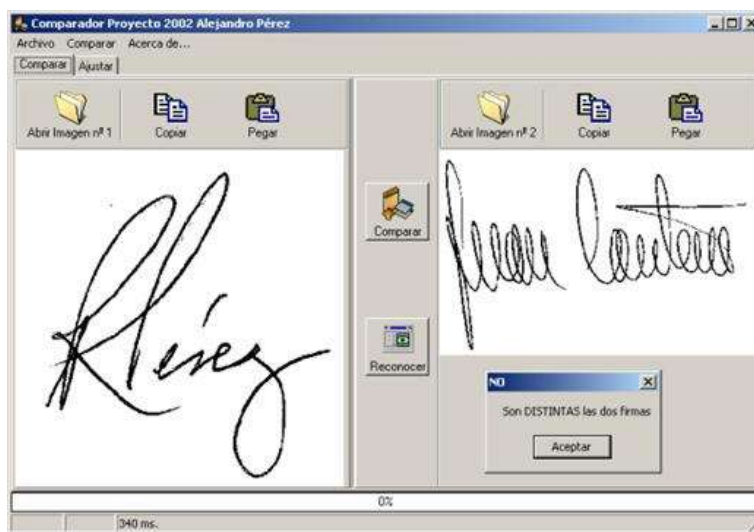


Ilustración 3. Captura de aplicación de firma manuscrita [6]

2.2.3 Voz

En esta técnica se toman las muestras de voz con un micrófono. Es un método de bajo coste y de fácil uso. Sin embargo, puede no ser muy fiable debido a cambios en la voz debido a factores como la edad, el estado de ánimo, la salud, etc. Por otro lado, no está totalmente demostrada la unicidad de la voz.

2.2.4 Rostro

Para ello, se toma una foto de la cara del sujeto en 2 o 3 dimensiones. Esta técnica aún no está completamente desarrollada. Tiene un coste bajo y es fácil de usar. Sin embargo, no es totalmente fiable debido a que existen personas con rasgos muy parecidos, como los gemelos, y por posibles cambios en la apariencia debido a heridas, cambios de peinado, etc.

2.2.5 Geometría de la mano

Se obtiene una imagen de la mano. Esta técnica no ha sido muy estudiada por el momento. Es de fácil uso y es aceptada por los usuarios. Sin embargo, no está comprobada la unicidad.

2.2.6 Dinámica de teclado

Esta técnica simplemente consiste en comprobar quién es un usuario dependiendo de la facilidad o rapidez con la que puede emplear un teclado. Se emplea fácilmente y es aceptada por los usuarios, pero la facilidad para usar un teclado puede depender del estado físico o anímico del sujeto y del teclado empleado.

2.2.7 Iris

Esta técnica consiste en la captura de una imagen del iris del sujeto. La unicidad es muy alta, por lo que es un método muy fiable. Sin embargo, el coste es muy alto y los individuos

sienten rechazo, además de ser de difícil empleo. En la ilustración 4 se pueden observar muestras de iris, en las cuales se puede ver las diferencias de características entre unas y otras.

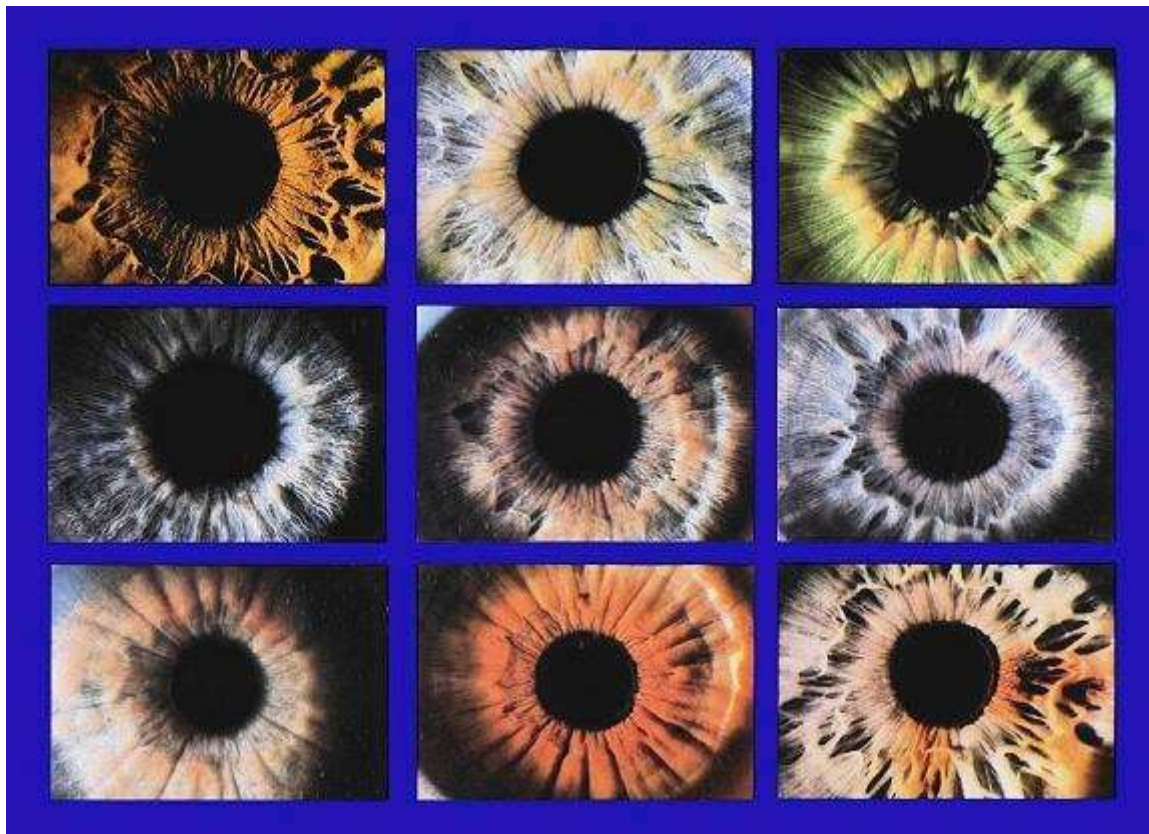


Ilustración 4. Muestras de iris [7]

2.2.8 Retina

Se toma una imagen del fondo de la retina para estudiar la capilaridad existente en la misma. Es una técnica altamente fiable, aunque el coste es muy alto y los usuarios no se encuentran cómodos con este tipo de reconocimiento.

2.2.9 Huella dactilar

Para llevar a cabo esta técnica, se toman imágenes de la huellas de un dedo. La fiabilidad es alta, pero tiene muchos inconvenientes como el rechazo de los usuarios debido a su uso policial, su coste en algunos casos y los problemas que ocasiona tomar algunas muestras. En la ilustración 5 se pueden ver un ejemplo de muestra de huella planar a la izquierda y otro de huella rodada a la derecha, que van a ser los dos tipos de huella empleados en este trabajo.



Ilustración 5. Muestras de huella dactilar [8]

2.3 Funciones de un sistema biométrico

Para llevar a cabo el proceso de identificación, la biometría hace uso de lo que habitualmente se conoce como sistemas biométricos. Estos sistemas deben realizar dos funciones bien diferenciadas:

- Reclutamiento: los usuarios deben permitir que se obtengan sus datos para generar un patrón que será característico de cada usuario.
- Comparación: se tomará una muestra del usuario y a partir de ella se obtienen los datos más significativos, es decir, lo que se conoce como vector de características. Posteriormente, se compara con los datos almacenados. Puede ser de dos tipos:
 - Verificación: este tipo de comparación se emplea cuando se pretende comprobar si un usuario es quien dice ser (comparación 1:1).
 - Identificación: esta forma de comparación se lleva a cabo cuando se quiere saber quién es el usuario que ha proporcionado sus datos (comparación 1:N).

Para poder realizar ambas funciones, el sistema realiza una serie de procesos. Dichos procesos se pueden observar en la Ilustración 2.

En el caso del reclutamiento, el primero de ellos es obtener la captura de la muestra biométrica. A continuación se llevará a cabo el pre-procesado en el que se elimina la información no útil. Más tarde, a partir de la muestra pre-procesada se extraen las características del individuo. Dichas características se almacenan en un fichero y esto es lo que se conoce como vector de características.

Para la verificación, el pre-procesado y la obtención del vector de características se realizan de la misma forma que en el reclutamiento. Posteriormente, se comparará el vector obtenido con el de su patrón correspondiente y se decide si se parece lo suficiente o no para dar la verificación como válida.

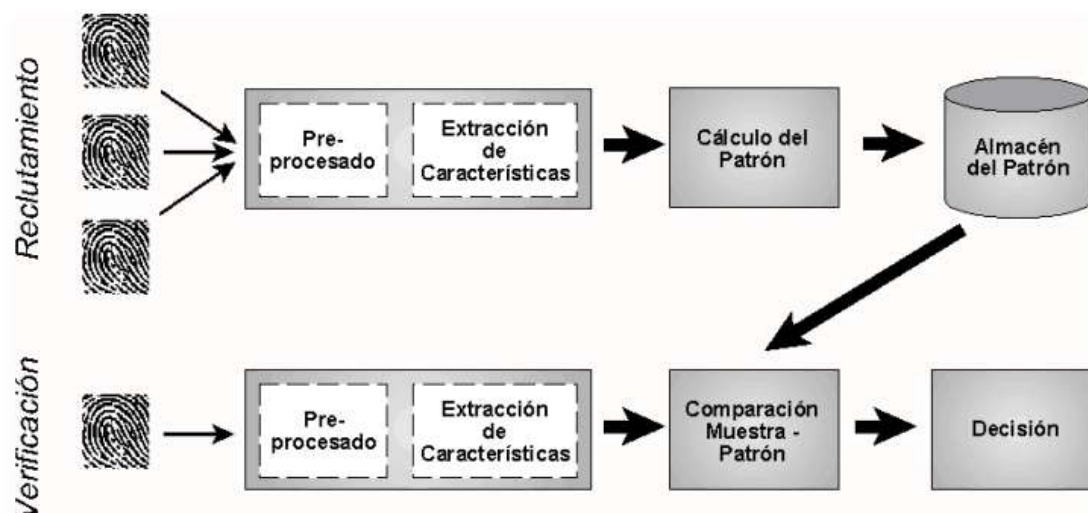


Ilustración 6. Fases del sistema biométrico [9]

2.4 Evaluación de los sistemas biométricos

La evaluación de los sistemas de identificación biométrica es compleja y depende de múltiples parámetros técnicos, sociológicos y económicos.

Dentro de todos estos parámetros hay que tener en cuenta factores como los mencionados en el apartado 2.2 respecto a las propiedades ideales que deberían cumplir las diversas modalidades, es decir, hay que analizar la universalidad, la unicidad, la estabilidad, la facilidad de captura de la muestra biométrica, su robustez frente al fraude, además de la aceptación por parte de los usuarios y su coste de implantación. Cabe destacar que de todos estos aspectos, los técnicos dependen del éxito o fracaso en la identificación del sujeto, mientras que los sociológicos y los económicos dependen en mayor medida de la aceptabilidad de este tipo de tecnología por parte del usuario [9].

Existen muchos tipos de evaluaciones, pero en el presente trabajo se van a utilizar la de rendimiento y la de interoperabilidad, que van a ser descritas a continuación.

2.4.1 Evaluación de rendimiento

La evaluación del rendimiento biométrico se encarga de estudiar el funcionamiento de los dispositivos, centrándose en la precisión y la rapidez. Pueden influir algunos parámetros como el entorno, el comportamiento del usuario, la interoperabilidad y la escalabilidad.

Los tipos de evaluación de rendimiento que puede haber son:

- **Tecnológica:** sirve para estudiar el rendimiento de algoritmos empleando una base de datos.
- **De escenario:** analiza el sistema biométrico teniendo en cuenta unas condiciones de entorno y tipo de población concretos.

- Operacional: se estudia el sistema biométrico en el entorno donde se va a emplear y con el tipo de población que lo va a utilizar.

Se pueden obtener medidas de rendimiento:

- Tasas de error: miden la precisión de un sistema para identificar personas.
 - FTE: indica una proporción de usuarios que no han podido completar el reclutamiento.
 - FTA: muestra una proporción de intentos de identificación en los que ha ocurrido algún error.
 - Verificación en comparación:
 - FNMR: proporción de muestras de usuarios genuinos que falsamente no coinciden con el patrón.
 - FMR: proporción de muestras de usuarios impostores que falsamente coinciden con el patrón.
 - Verificación del sistema completo:
 - FRR: transacciones incorrectamente denegadas.
 - FAR: transacciones de impostor incorrectamente aceptadas.
 - GFRR: mide el rendimiento según los usuarios rechazados.
 - GFAR: mide el rendimiento según los usuarios impostores aceptados.
 - Identificación para el sistema completo:
 - FNIR: transacciones de identificación para usuarios reclutados para los cuales no se devuelve el identificador correcto en la lista de candidatos.
 - FPIR: transacciones de identificación para usuarios no reclutados para los cuales no se devuelve una lista de candidatos vacía.
 - Identification rate: transacciones de identificación para usuarios reclutados para los cuales se devuelve el identificador correcto en la lista de candidatos.
 - Curvas de rendimiento
 - ROC: compara 1-FNMR y la FMR. Se puede ver un ejemplo en la Ilustración 7.

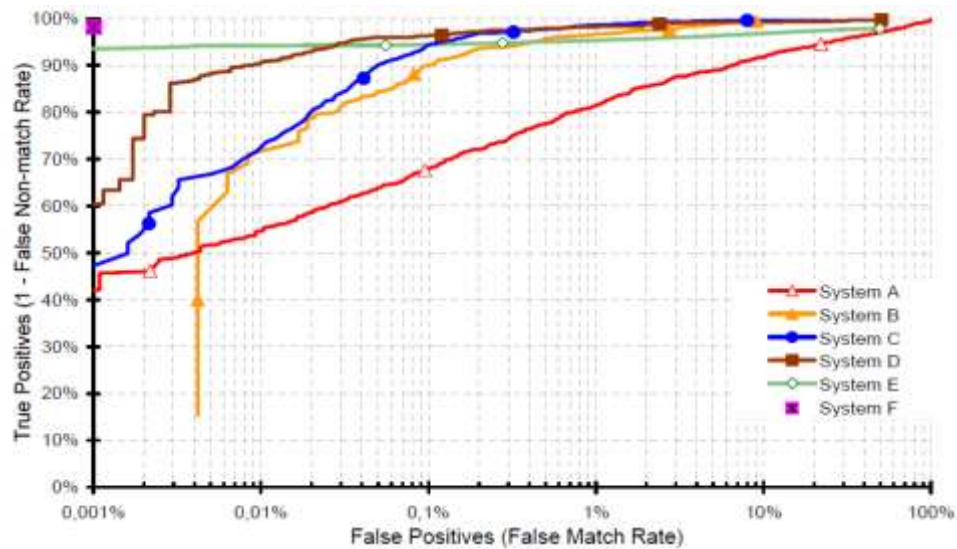


Ilustración 7. Curva ROC [10]

- DET: compara la FNMR y la FMR. Se puede ver un ejemplo en la Ilustración 8.

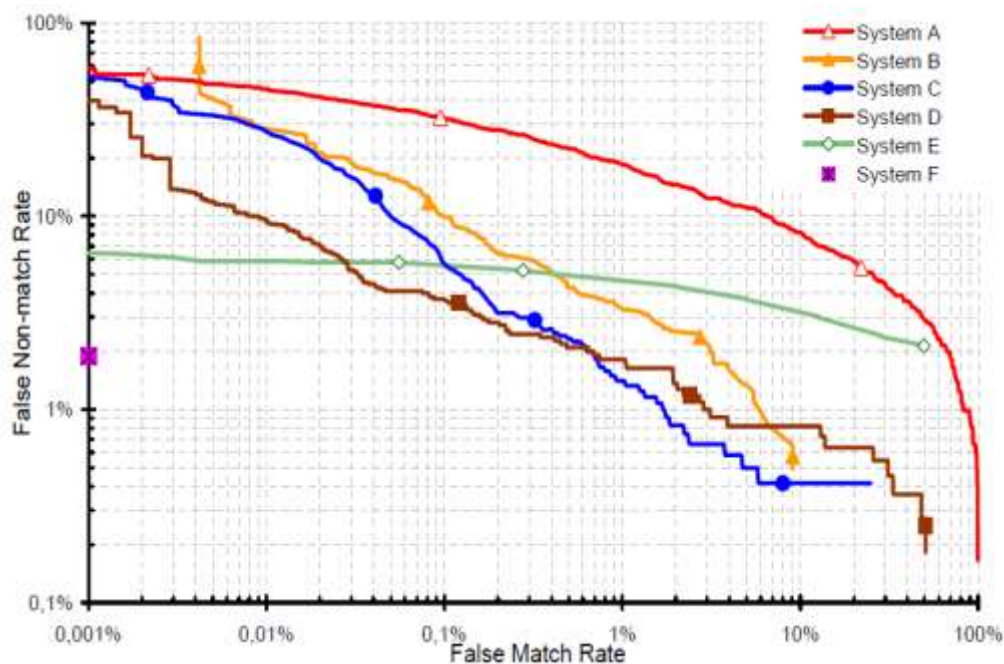


Ilustración 8. Curva DET [10]

- EER: tasa de igual error. Punto en el que la FNMR/FMR o FRR/FAR tienen el mismo valor. Se puede observar un resultado en la siguiente figura.

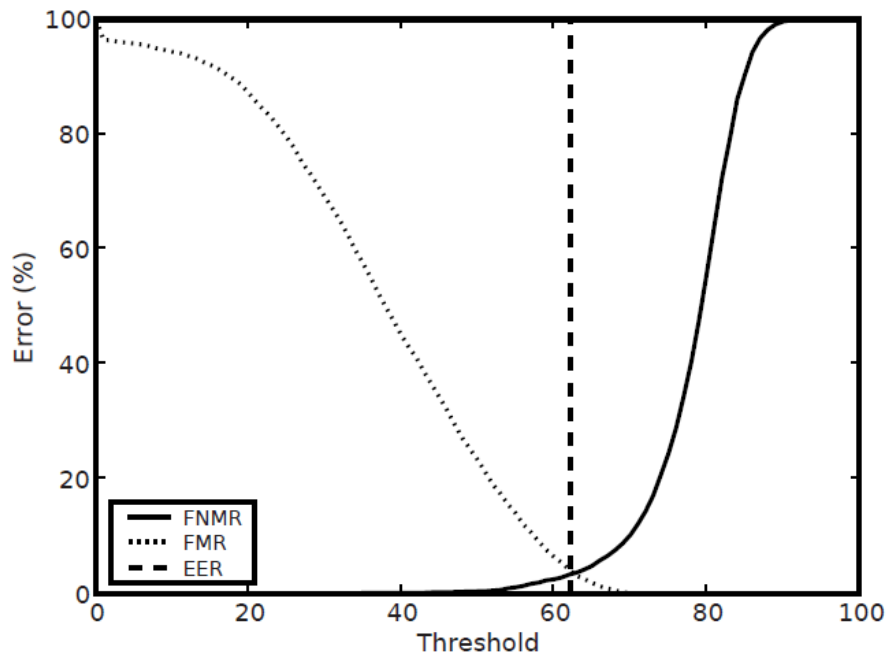


Ilustración 9. Curvas FNMR vs FMR [10]

- Tasas de throughput: miden el número de usuarios que puede procesar el sistema en una unidad de tiempo. Se debe definir entre qué instantes se va a dar dicha unidad de tiempo. Se utilizan la media aritmética, mínimo, máximo y desviación típica. [10]

2.4.2 Interoperabilidad

Para el presente TFG es importante definir el concepto de interoperabilidad, que consiste en evaluar el rendimiento de los sistemas cuando las muestras o los patrones han sido generados por otros sistemas biométricos.

Para poder compartir datos entre distintas organizaciones y que no sea necesario emplear siempre los mismos dispositivos, se comenzaron a desarrollar estudios sobre la interoperabilidad de los dispositivos biométricos.

Debido a que no se conseguían los mismos resultados con unos dispositivos que con otros, se establecieron unos criterios para que los datos tuvieran un formato estándar de interoperabilidad.

Se establecen dos requisitos para evaluar el rendimiento:

- Si son sistemas que utilizan datos con formato estándar, presentan el mismo rendimiento que aquellos que utilizan formatos propietarios.
- Si es un sistema de fabricante específico, tiene el mismo rendimiento si utiliza los datos biométricos con un formato estándar generados por otro fabricante que los que genera él mismo.

Se debe determinar cómo se lleva a cabo la interoperabilidad entre los diferentes sistemas biométricos, para luego llevar a cabo las pruebas y calcular las tasas de rendimiento, dependiendo de la configuración y de la forma en que se produce la interoperabilidad. [11]

Para este trabajo, se ha realizado una evaluación de interoperabilidad teniendo en cuenta el segundo de los requisitos, es decir, se analiza el rendimiento de un dispositivo de huella planar si el reclutamiento se ha realizado con un dispositivo de huella rodada, y viceversa.

Para ello, se van a llevar a cabo una serie de pruebas que serán explicadas en detalle en el apartado 5.

3 Diseño

A continuación se van a detallar las aplicaciones y los elementos necesarios para conseguir realizar pruebas que indiquen el rendimiento de dos tipos de sistemas biométricos, de huella planar y de huella rodada.

3.1 Diseño de la aplicación

3.1.1 Requisitos generales

Para cumplir con los objetivos planteados en este TFG, ha sido necesario desarrollar dos aplicaciones. Dichas aplicaciones se describen a continuación.

- Obtención de minucias y valores de comparación:

Es una aplicación, desarrollada mediante Visual Studio y empleando el lenguaje C#, que permite obtener los vectores de características de cada una de las muestras elegidas de una base de datos para posteriormente obtener los valores de comparación entre dichas muestras.

- Obtención de tasas de rendimiento:

Esta aplicación ha sido desarrollada utilizando el programa MATLAB. Gracias a ella, se ha conseguido obtener unas gráficas que muestran los resultados de las tasas de rendimiento de los distintos dispositivos de huella dactilar a partir de los resultados obtenidos en la aplicación de obtención de minucias y valores de comparación.

3.1.2 Requisitos específicos

3.1.2.1 *Requisitos para el análisis de las muestras*

Para el desarrollo de la primera de las aplicaciones mencionadas en el apartado anterior, es necesario tener en cuenta una serie de parámetros, ya que el objetivo de esta aplicación es poder realizar las comparaciones oportunas en función de cuáles de estos parámetros sean seleccionados:

- Distintos Sensores

Se han empleado distintos sensores que serán detallados más adelante. Todos ellos se han utilizado en modalidad planar y uno de ellos además en rodada.

- Diferentes fases del proceso de identificación: Reclutamiento o verificación

Se han llevado a cabo fases de reclutamiento y de verificación. De este modo, en el reclutamiento se han obtenido huellas que han sido empleadas como patrón, mientras que en la verificación se han conseguido huellas que han sido comparadas con los patrones para poder identificar a los usuarios. La aplicación permitirá elegir qué sensor usar en cada una de estas fases.

- Varias visitas para la verificación

Se han realizado 3 visitas para poder obtener 3 muestras distintas para realizar la comparación. De este modo, se ha podido tener en cuenta factores como el tiempo, estado de ánimo, heridas, etc. La aplicación permitirá elegir qué visitas se van a tener en cuenta para el experimento.

- Ruta en la que se encuentra la base de datos

La aplicación deberá ser capaz de ofrecer la opción de seleccionar en qué carpeta se encuentran las muestras que se van a emplear para la prueba que se va a llevar a cabo, ya que dependiendo del experimento se van a requerir unas muestras u otras.

- Ruta para almacenar los vectores de características

La aplicación debe permitir al usuario elegir en qué directorio guardar los vectores de características obtenidos. De esta forma, se puede almacenar los resultados de distintos experimentos en carpetas diferentes.

- Ruta para almacenar los valores de comparación

Al igual que con el requisito anterior, la aplicación permitirá que el usuario pueda elegir la ruta donde almacenar los resultados de la comparación, ya que estos resultados serán empleados más adelante para calcular las tasas de rendimiento.

- Rango de usuarios

El programa permite elegir que usuarios van a formar parte del experimento, para poder hacer distintos análisis.

Además, ha sido de gran utilidad esta opción ya que ha permitido realizar pruebas sin procesar la base de datos completa.

- Recopilación de vectores de características y resultados del proceso

A partir de las muestras tomadas, la aplicación obtendrá los vectores de características para posteriormente comparar unos con otros y obtener los valores de comparación, que serán necesarios para calcular las tasas de rendimiento.

3.1.2.2 Requisitos para el análisis del rendimiento

Tras obtener los resultados de las comparaciones que produce la primera aplicación, la segunda deberá procesar estos resultados para calcular las medidas de rendimiento de los sistemas biométricos y mostrarlas al usuario. Los requisitos que debe cumplir esta aplicación son los siguientes:

- Rutas donde se encuentren los valores de comparación

La aplicación permitirá al usuario poder elegir las rutas donde se encuentren los valores de comparación de dos experimentos ya que, como se ha explicado anteriormente, ha podido elegir donde almacenarlos.

- Obtención de tasas FMR y FNMR

A partir de los resultados de comparación, la aplicación obtendrá los valores de FMR y FNMR que permiten obtener las gráficas FAR vs FRR, ROC y DET, ya que estas gráficas dependen de los valores mencionados, como se explicó en el apartado 2.

- Gráficas de comparación

Por último, la aplicación obtendrá las gráficas FAR vs FRR, ROC y DET de dos tipos de consulta realizadas por el usuario, que se explicarán en detalle más adelante. Estas gráficas permiten poder comparar los resultados de una consulta con otra.

3.2 Herramientas necesarias

Las principales herramientas empleadas han sido la base de datos de huellas dactilares, el software de desarrollo y los algoritmos del NIST. En este apartado se van a explicar detalladamente.

3.2.2 Base de datos

La base de datos es un elemento fundamental para este trabajo. Hay que tener en cuenta los sensores utilizados para su captura, la aplicación que ha sido utilizada, el procedimiento empleado y la composición de la base de datos. Por ello, a continuación van a ser descritos dichos puntos.

3.2.1.1 Sensores

La base de datos utilizada en este TFG ha sido recogida utilizando 4 sensores distintos de huella dactilar. A continuación se van a describir brevemente las características de cada uno de ellos y su funcionamiento.

- **SupremaBioMini**



Ilustración 10. Sensor Suprema BioMini [12]

Este sensor óptico tiene un funcionamiento muy sencillo. Simplemente basta con apoyar la superficie central del dedo en el cristal durante aproximadamente tres

segundos. Se enciende una luz azul que se puede ver, a través del cristal, cuando el sensor puede usarse y se apaga cuando se retire el dedo.

- **SecuGen Hamster IV**



Ilustración 11. Sensor SecuGen Hamster IV [13]

Este sensor óptico tiene un funcionamiento parecido al anterior, sólo es necesario apoyar el dedo. Al hacerlo, se enciende una luz roja visible a través del cristal, que se apaga cuando la muestra haya sido tomada. Es entonces cuando el usuario puede apartar el dedo del sensor.

- **Suprema RealScan-D**



Ilustración 12. Sensor Suprema RealScan-D [14]

Este es un sensor óptico que se ha podido utilizar para dos tipos de capturas distintas. Una de ellas es la de posada de dos dedos. Para ello, sólo hay que apoyar los dedos índice y corazón a la vez en el sensor. Habrá que hacerlo cuando aparezca una luz verde a través del cristal y quitar ambos dedos cuando el dispositivo reproduzca el sonido de un pitido.

Por otro lado, también se ha hecho una captura de huella rodada, bastante más complicada. Al encenderse la luz, el usuario debe apoyar el lateral del dedo. Tras producirse un pitido, se debe rodar el dedo y posteriormente levantarlo. Si la captura es exitosa, al levantar el dedo pita una vez. En caso contrario, pita 3 veces seguidas.

- **Upek Eikon Fingerprint Reader**








Ilustración 13. Sensor Upek Eikon Fingerprint Reader [15]

El empleo de este sensor semiconductor consiste en arrastrar toda la superficie de la yema del dedo apoyándolo en la dirección y sentido que indica la flecha. Si se detecta el dedo, se enciende la luz azul de la parte baja.

Los resultados que se pueden obtener en los distintos sensores pueden ser, por ejemplo, los que se muestran en la Tabla 1.

Tabla 1. Ejemplos de huellas

SupremaBioMini	SecuGen Hamster IV	Suprema RealScan-D Modo rodada	Suprema RealScan-D Modo posada	Upek Eikon Fingerprint Reader
				

3.2.2.2 Aplicación y procedimiento de recopilación de muestras

Se ha empleado un programa que ha permitido hacer una recopilación de las muestras de los usuarios. Dicho programa permite realizar dos fases, una para el reclutamiento del individuo, en la cual se toman dos muestras de cada huella dactilar, y otra de reconocimiento, en la que se comparan las muestras tomadas en dicho momento con las obtenidas en el reclutamiento de dicho usuario para el mismo dedo. En la ilustración se puede observar la pantalla principal de la aplicación.



Ilustración 14. Pantalla principal de la aplicación de huella

En la primera visita, se explicaba al usuario todo el proceso y se tomaban sus datos personales, entre ellos si el usuario tiene enfermedades de la piel o si no dispone de algún dedo. A continuación se muestra la pantalla que aparece con los datos que se deben rellenar.



Ilustración 15. Pantalla para recopilación de datos personales

Posteriormente, el usuario tenía que pasar por una fase de reclutamiento en la que disponía de 5 oportunidades para registrar su huella dactilar, que debe tener dos muestras que coincidan entre sí.




Los errores que se podían producir en el reclutamiento de la huella dactilar son muy variados. Se podían producir problemas debido a una mala interacción del usuario, al usar el sensor de manera errónea. También podía haber problemas si la huella estaba más seca de lo normal, en cuyo caso se aconsejaba al usuario que se tocara la frente con el dedo. Si la huella estaba más húmeda, el usuario debía secarse el dedo con un pañuelo o con la ropa. En los casos de huella húmeda, la imagen se veía más oscura y era difícil reconocer los rasgos. En los de huella seca ocurría al contrario, la imagen era demasiado clara y no se lograba ver bien las líneas. Además, se podían producir

problemas debido a que la calidad de la muestra tomada fuera baja, si el usuario desplazaba el dedo en una dirección errónea, si la huella era corta debido a que no se tomase toda la superficie que se debía tomar o si el individuo se equivocaba en el dedo que tenía que colocar.

En caso de que el programa admitiera la muestra pero no se viera convenientemente, se debía repetir la toma de la huella.

En la Tabla 2 se puede observar ejemplos de errores.

Tabla 2. Ejemplos de errores

Huella de poca calidad	Huella corta	Huella seca
		

Hay que mencionar que cuando se agotaban los intentos para conseguir la muestra de una huella se producía un error FTE, por lo que ese dedo se quedaba sin reclutar. A continuación se muestra la pantalla que anuncia este error.



Ilustración 16. Error de FTE

También era necesario tener cuidado con el tiempo que se tardaba en tomar una muestra, ya que si se agotaba el periodo establecido se producía un error de “Timeout”. A continuación se puede observar el mensaje de este error.



Ilustración 17. Error de “Timeout”

A continuación se muestra la pantalla de reclutamiento.



Ilustración 18. Pantalla de reclutamiento

En caso de que dos muestras no coincidan entre sí, se dará al operario de huella la opción de comenzar de nuevo el reclutamiento para ese dedo, eliminar la segunda muestra o abortar el reclutamiento de ese dedo. Se puede observar en la siguiente imagen.



Ilustración 19. Pantalla que compara dos muestras tomadas

A continuación, se debía realizar la fase de reconocimiento en la que se comparaban las muestras con las obtenidas en el reclutamiento. En la segunda visita, sólo se realizaba esta fase. Por último, en la tercera visita se realizaba la fase de reconocimiento y se proporcionaba un cuestionario de satisfacción al usuario.

En esta fase, inicialmente se muestra una ventana para elegir cuál es la visita que se va a realizar, tal y como se muestra a continuación.

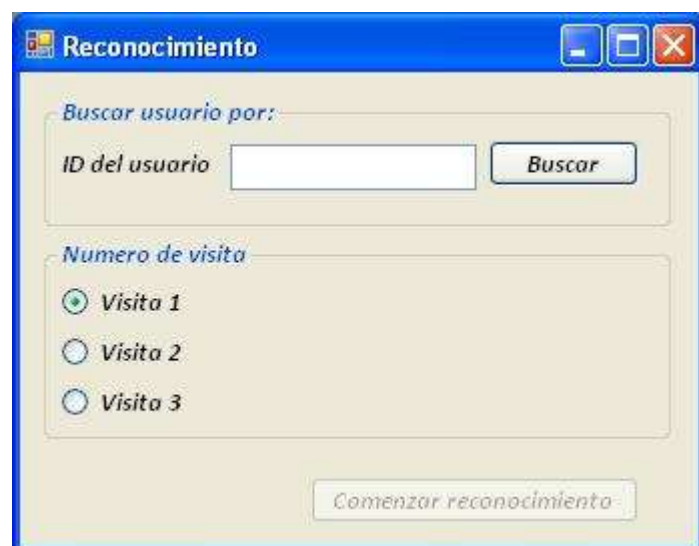


Ilustración 20. Pantalla de elección de visita

Se deben tomar 4 muestras para cada dedo, exitosas o erróneas. Para cada una de estas muestras, se dispone de 3 oportunidades para tomar una huella correcta. Para que no haya errores, se debe adquirir una muestra en la cual coincidan sus características con las de la huella tomada en el reclutamiento. Además, se debe tener un mínimo de calidad en dicha muestra para ser válida. Sólo se realizaba la fase de reconocimiento para aquellos dedos que habían podido ser reclutados previamente.

Cuando se superaban los intentos para reconocer un dedo, se producía un error FTA y se continuaba con el reconocimiento. A continuación se muestra la pantalla de error FTA.



Ilustración 21. Pantalla de error FTA

A continuación se muestra la pantalla de reconocimiento.



Ilustración 22. Pantalla de reconocimiento

Como se ha podido observar en las ilustraciones, en ambas fases se muestra una imagen de dos manos con un círculo rojo alrededor de uno o dos dedos indicando qué dedo o dedos se deben utilizar en ese momento y el número de intentos consumidos por el usuario. En el caso del reconocimiento, también se muestra el número de muestras ya tomadas.

Todo se guarda en una base de datos. Se almacenan las imágenes de las huellas dactilares tomadas, el fichero con los datos para identificar al usuario y otro fichero con los errores que se hayan producido durante la toma de las muestras.

En este programa, al individuo sólo se le identifica con un número de usuario. Los demás datos personales se encuentran en el fichero correspondiente.

3.2.2.3 *Base de datos final y opinión de los usuarios*

En general, los usuarios que han acudido a las visitas han sido los miembros del Grupo o alumnos de la universidad. Esto ha hecho posible que el número de usuarios que estén habituados al uso de sistemas biométricos y los que no lo están haya sido equilibrado. De esta forma se elimina la posible influencia de este factor en los resultados.

En concreto se obtuvieron datos de 72 usuarios, de los cuales 67 acabaron el proceso de captura de huellas. De esos 72 usuarios, 56 son hombres y 16 mujeres. 50 personas son menores de 30 años, 16 mayores de 30 y menores de 50 años y 6 mayores de 50. 64 usuarios son diestros y 8 zurdos.

Durante la captura de huellas, se ha podido observar las preferencias y los problemas con los que se han encontrado los usuarios. La mayor parte de ellos han tenido grandes problemas con el sensor Suprema RealScan-D, concretamente en el modo de huella rodada. Esto es debido a que girar el dedo supone un esfuerzo al tener que mover toda la muñeca o incluso el cuerpo. Además, su gran tamaño lo hace poco manejable. Por ello, se producía un gran número de errores con este sensor debido a la interacción errónea del usuario.

El modo de huella posada es mucho más sencillo, rápido y cómodo, siendo uno de los que más ha gustado entre los individuos.

En cuanto al sensor Suprema BioMini, las conclusiones son bastante diferentes. Los usuarios no tenían problemas generalmente debido a su facilidad de uso y a su pequeño tamaño que lo hace más manejable. La única pega es que no está dotado de ningún tipo de aviso para informar al usuario de que la huella ya ha sido capturada.

Por otro lado se encuentra el sensor SecuGen Hamster IV, que tiene unas características parecidas al sensor anteriormente descrito. Además, su forma se adapta a la mano para tener una mayor facilidad de uso. Algo positivo que tiene este sensor es que la luz roja avisa cuando se apaga de que ya ha sido tomada la muestra. Sin embargo, había gente que debido a que el tamaño de su dedo era grande no podía ver con facilidad esta luz, provocando algunas dificultades.

Por último, el sensor Upek Eikon Fingerprint Reader no ha tenido mucho éxito entre los usuarios, debido a que les resultaba un poco incómodo de utilizar al tener que deslizar el dedo por la superficie del sensor. Se producían muchos errores de huella corta ya que no se apoyaba bien el dedo. También podían ocurrir errores en la dirección del dedo, ya que se debía arrastrar en línea recta.

Cabe destacar los problemas encontrados en algunos usuarios al usar los sensores simplemente por la calidad de las muestras tomadas. Los dispositivos tomaban sus

huellas dactilares con una calidad que era bastante inferior a la que se necesitaba para que el programa las aceptara como válidas. Esto ha provocado alargar bastante el tiempo empleado en el reclutamiento debido a que ha sido necesario repetir las tomas de huellas numerosas veces, hasta agotar los intentos. Este suceso ha significado perder bastantes muestras en la fase de reclutamiento.

3.2.3 Herramientas de software

Para desarrollar las aplicaciones, han sido necesarias dos herramientas: Visual Studio y Matlab.

3.2.2.1 *Visual Studio*

Visual Studio es un programa soportado por el Sistema Operativo Windows. Se pueden emplear distintos lenguajes de programación como Visual C++, Visual C#, Visual J# y Visual Basic .NET. Permite crear aplicaciones además de servicios web en entornos que soporten la plataforma .NET. [16]

3.2.3.2 *Matlab*

Matlab es un programa que permite llevar a cabo cálculos numéricos de todo tipo. Tiene un lenguaje de programación propio. Entre sus funciones, se pueden nombrar el uso de matrices, funciones, algoritmos, la creación de interfaces de usuario y la comunicación con otros programas escritos en otros lenguajes. Contiene dos herramientas llamadas Simulink, que permite realizar simulaciones, y GUIDE, que es un editor de interfaces de usuario. [17]

3.2.4 Algoritmos del NIST

Además, para obtener los resultados se han empleado dos algoritmos creados por el NIST.

3.2.4.2 *Detector de minucias y extracción del vector de características*

Para realizar la detección de minucias y la extracción del vector de características, se ha empleado una herramienta que proporciona el NIST denominada mindtct. Este algoritmo procesa una imagen y detecta las minucias. Los puntos característicos se almacenan en los vectores de características. [18] También evalúa la calidad de la muestra según las condiciones de la imagen. [19]

3.2.4.3 *Algoritmo de comparación*

Para realizar la comparación entre las muestras y el patrón se ha empleado el algoritmo de comparación denominado Bozorth. Este algoritmo basa su funcionamiento en conseguir la coincidencia entre minucias de las huellas dactilares sin tener en cuenta la posición y orientación de dichas huellas. Acepta minucias generadas por el algoritmo mindtct. [19]

4 Desarrollo

Para llevar a cabo el estudio de las tasas de rendimiento para los distintos dispositivos de huella dactilar, han sido realizados dos programas para llegar a cumplir dichas acciones, como ya se ha mencionado anteriormente. En este apartado se explican detalladamente dichas aplicaciones y su funcionalidad.

4.1 Obtención de minucias y valores de comparación

En primer lugar ha sido desarrollada una aplicación mediante la plataforma Visual Studio, empleando el lenguaje de programación C#.

En la imagen siguiente se puede observar el aspecto de la pantalla que se muestra al usuario al ejecutar el programa. Su interfaz permite al individuo realizar distintas ejecuciones según su necesidad, ya que dispone de múltiples campos de entrada que cumplen con los requisitos explicados en el apartado de diseño.

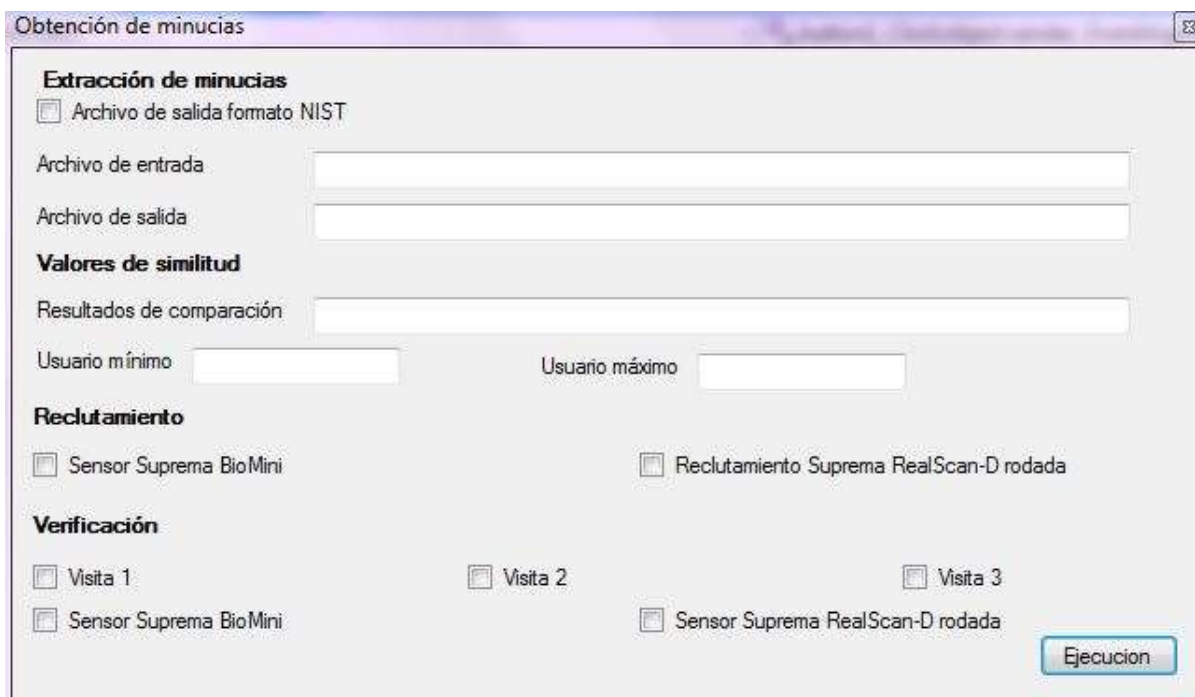


Ilustración 23. Pantalla de la aplicación de valores de comparación

El algoritmo para detectar las minucias y obtener el vector de características permite dos formatos. Por ello, se ha creado la opción de usar el formato NIST, que es un estándar que define la forma de especificar y compartir las coordenadas de geoposicionamiento de las muestras biométricas para conseguir una mayor fiabilidad a la hora de identificar a un

individuo [20]. Sin embargo, dado que el algoritmo de comparación requiere que se use este formato, es aconsejable seleccionar esta opción.

A continuación se muestra una imagen que muestra la opción marcada.

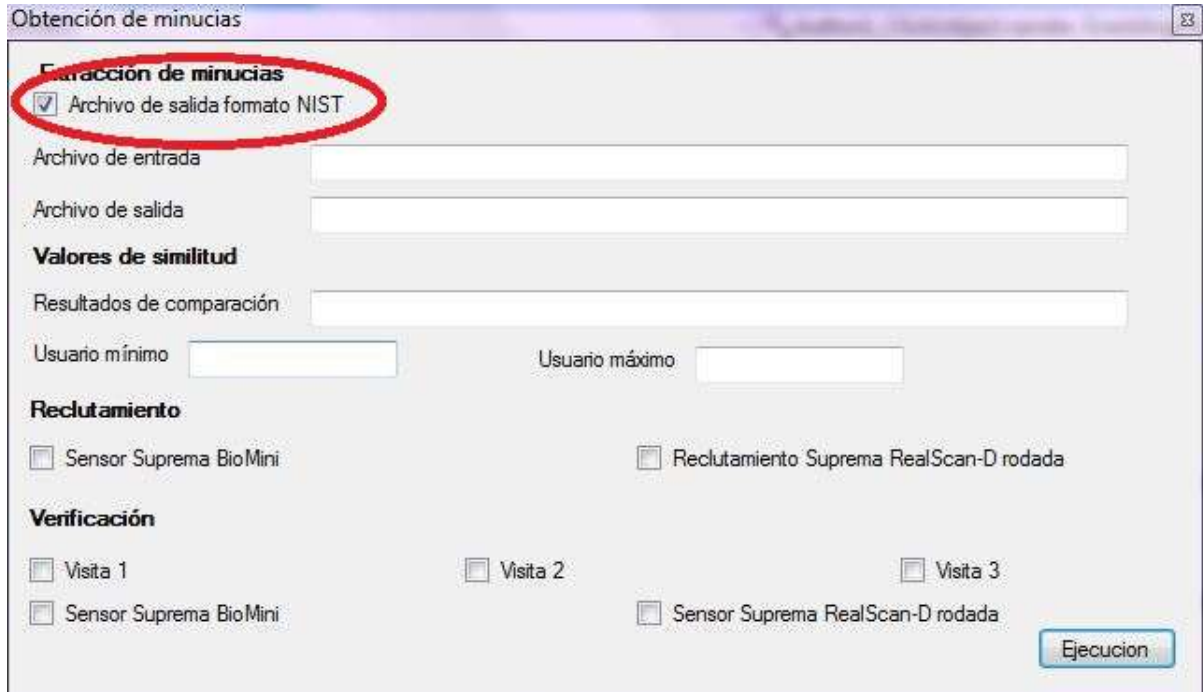


Ilustración 24. Pantalla con la opción formato NIST

Posteriormente, el usuario debe introducir la ruta de los archivos de entrada, que será la base de datos obtenida, dentro de la cual se haya una subcarpeta para cada usuario que contendrá las imágenes que representan las huellas dactilares obtenidas.

También debe introducirse la ruta donde se quieren almacenar los resultados, es decir, los vectores de características de cada una de las imágenes de la base de datos.

A continuación se muestra un ejemplo.

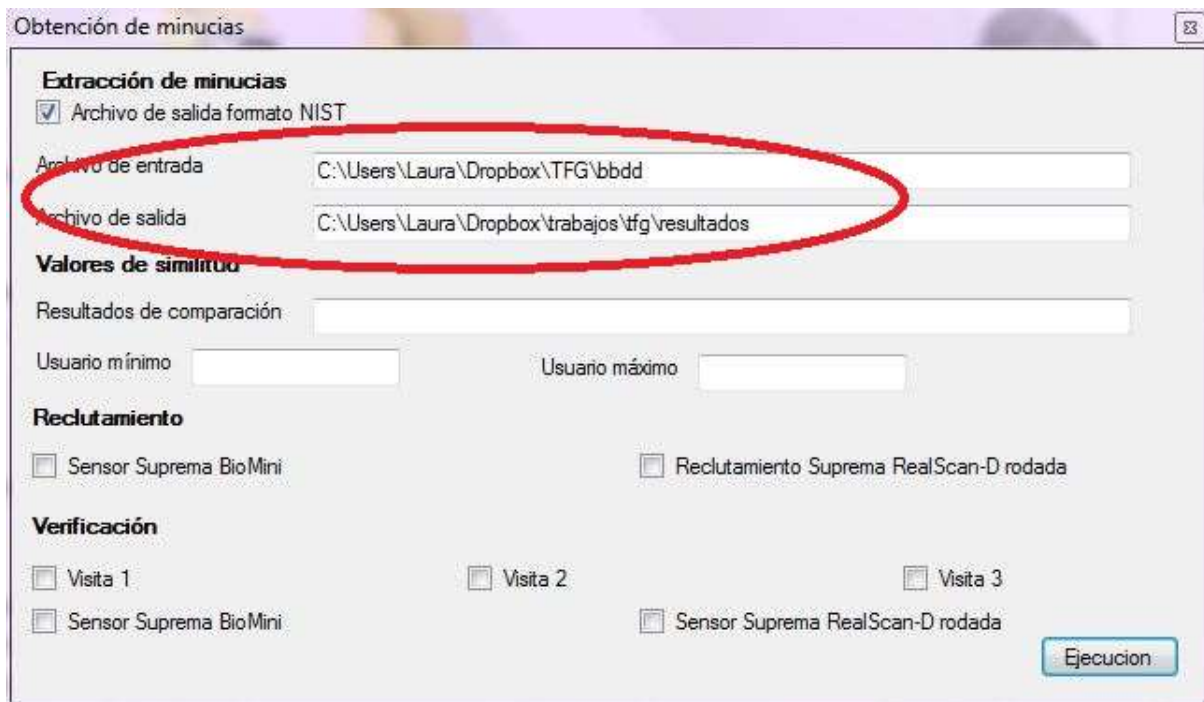


Ilustración 25. Pantalla introduciendo rutas para extracción de minucias

También es necesario especificar la ruta en la que se van a almacenar los valores de similitud, como se puede comprobar en la siguiente imagen.

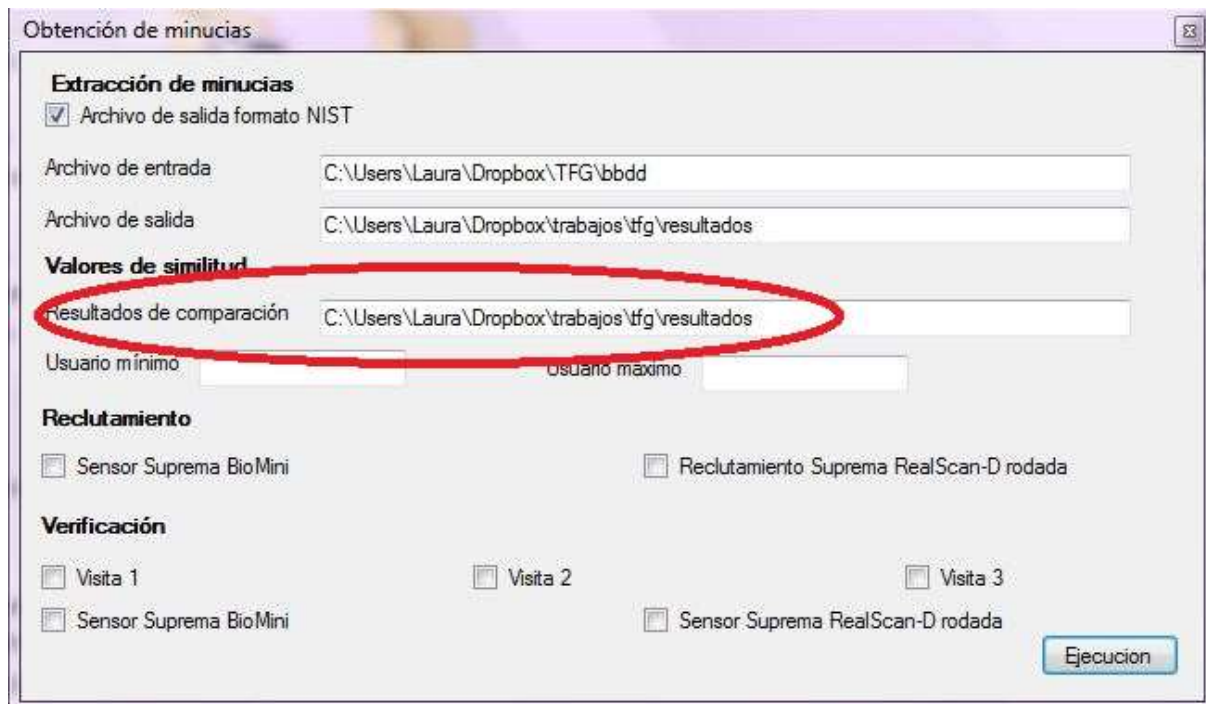


Ilustración 26. Pantalla introduciendo ruta de salida de valores de similitud

Además hay que elegir el rango de usuarios que se van a usar para obtener los resultados. Esto se consigue introduciendo el valor del usuario con identificador más bajo y el del más alto, como se muestra en la imagen siguiente. Tal como se comentó en los requisitos de la aplicación, esta función ha sido útil para realizar las pruebas de manera más rápida.

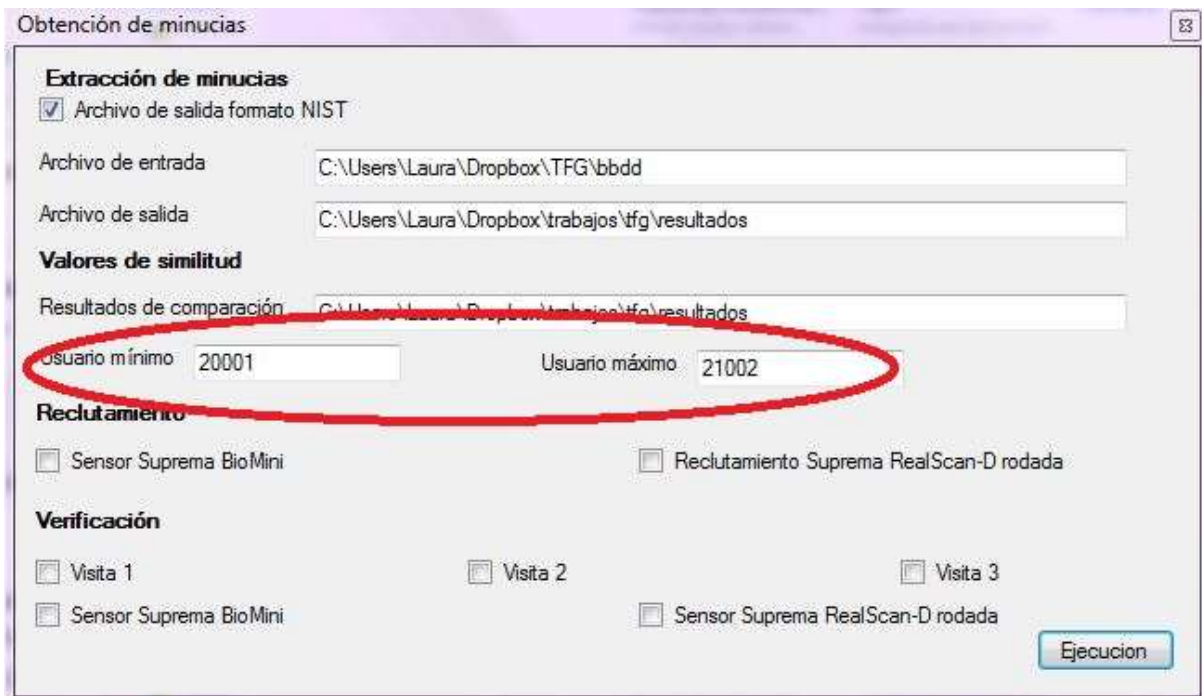


Ilustración 27. Pantalla introduciendo los usuarios mínimo y máximo

Posteriormente, es necesario seleccionar cuál de los dispositivos de huella ha sido empleado en el reclutamiento. A pesar de que la base de datos ha sido recogida empleando 4 dispositivos, para este trabajo sólo es necesario el uso de un dispositivo de huella planar y otro de huella rodada, por lo que se han escogido el sensor Suprema BioMini y el sensor Suprema RealScan-D rodada.

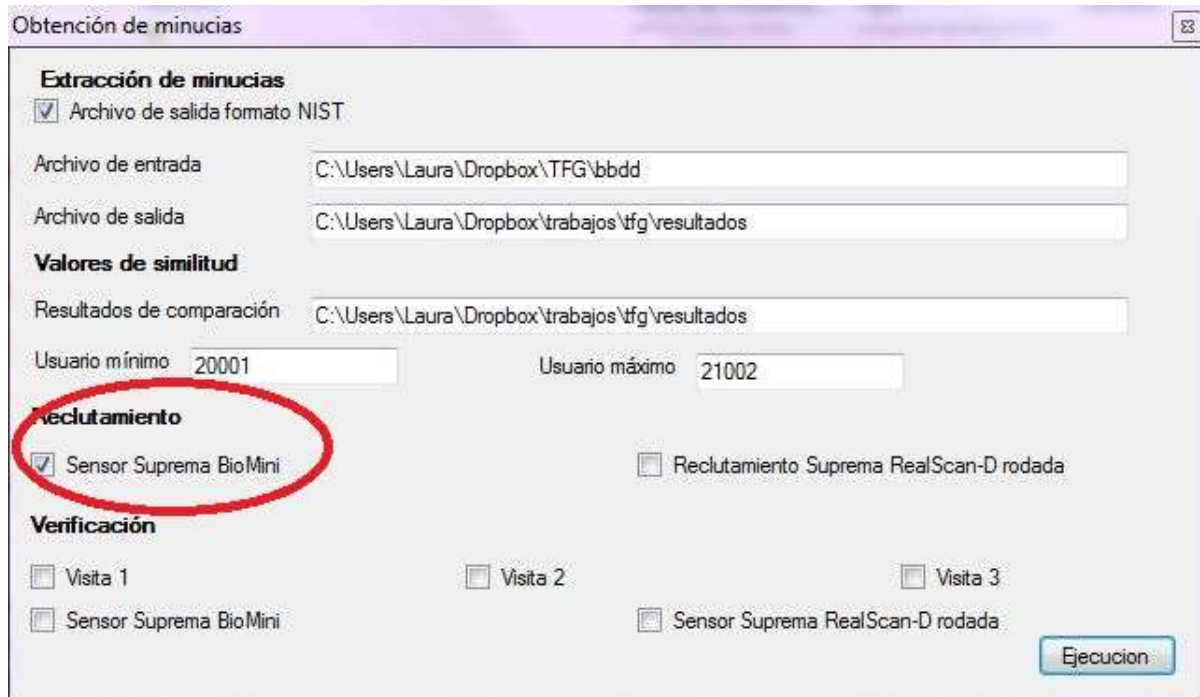


Ilustración 28. Pantalla de elección de dispositivo de reclutamiento

Por último, es necesario seleccionar las visitas que se van a tener en cuenta de la verificación, además del dispositivo que se va a usar, como se puede observar a continuación.

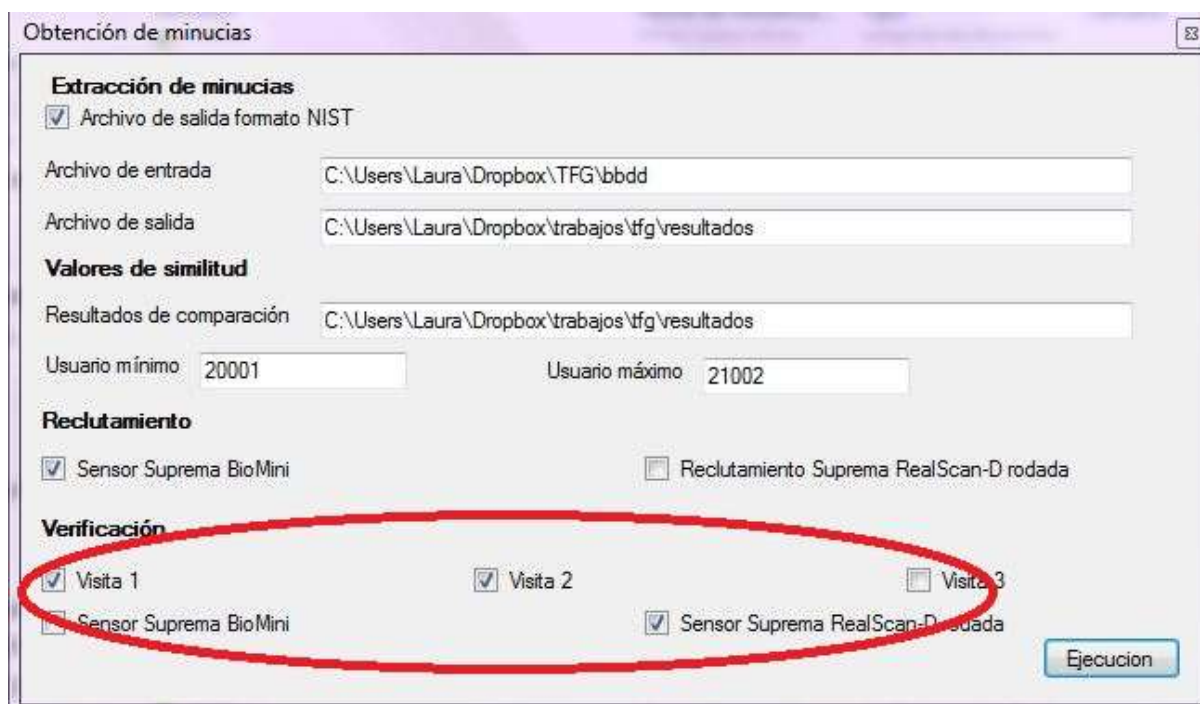


Ilustración 29. Pantalla de elección de visitas y dispositivo de verificación.

En cuanto al funcionamiento del programa, a partir de la base de datos completa, sólo se van a utilizar aquellas imágenes que cumplan con los requisitos introducidos por el usuario, es decir, el número de usuario, las muestras que hayan sido reclutadas con el sensor especificado y las que hayan sido realizadas en la verificación en las visitas elegidas y con el sensor seleccionado. A partir de estas imágenes, se obtienen las minucias de cada una de ellas que se almacenan en ficheros .XYT. Para almacenar estos ficheros, se guardan los que correspondan a imágenes obtenidas en el reclutamiento en una carpeta de patrones y los archivos que correspondan a imágenes de la verificación en una carpeta de muestras. Estas carpetas son creadas en la ruta especificada por el usuario como “Archivo de salida”.

Posteriormente, se realizan comparaciones genuinas y de impostor. Las comparaciones genuinas se realizan entre cada muestra y su patrón obtenido en el reclutamiento, mientras que las de impostores se deben realizar entre cada muestra y cada patrón que no es el suyo propio. Por ello, para saber si se va a realizar una comparación de genuinos o impostores, se debe comparar el nombre de cada archivo de reclutamiento con los archivos de verificación. En caso de que el número de usuario y el dedo del que se haya obtenido la muestra sea el mismo, la comparación será de genuinos. En caso contrario, la comparación será de impostores. La estructura del nombre de un archivo es la siguiente:

Número de usuario + dedo + mano derecha o izquierda + tipo de sensor + reclutamiento o número de visita + número de muestra.

Por ejemplo, 20001CDSRE013.bmp

Por tanto, para ser genuinos deben coincidir en los 7 primeros caracteres, mientras que para ser impostores no debe haber una coincidencia exacta en los 7 primeros caracteres.

Posteriormente, se ha empleado el ejecutable bozorth3.exe para conseguir los valores de comparación.

Los valores de comparaciones genuinas se almacenan en el fichero BOZ_gen.txt, mientras que los valores de comparaciones de impostor se guardaran en el fichero BOZ_imp.txt. Estos ficheros son creados en la ruta especificada por el usuario como “Resultados de comparación”. La estructura de estos ficheros es una matriz en la que cada fila contiene el nombre de las dos muestras a comparar y su valor de comparación.

4.2 Obtención de tasas de rendimiento

El segundo programa ha sido creado en MATLAB. A continuación se puede ver la pantalla que se muestra al usuario al ejecutar.

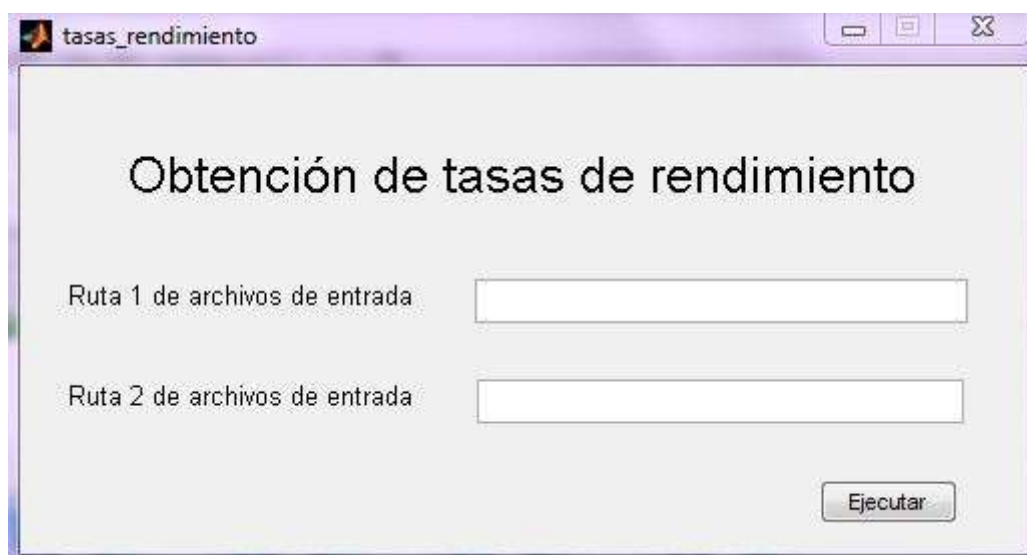


Ilustración 30. Captura de pantalla de la aplicación para tasas de rendimiento

El objetivo de esta aplicación es obtener los resultados de rendimiento para diferentes combinaciones de sensores y modos de adquirir las muestras y poder compararlos, como ya se ha mencionado en el apartado 3.

Por esta razón y como se puede observar, el programa ofrece al usuario la posibilidad de indicar dos rutas de datos distintas. Cada una de ellas se corresponderá con una evaluación de rendimiento en concreto. En cada una de estas rutas deben encontrarse los ficheros BOZ_gen.txt y BOZ_imp.txt con los resultados de haber realizado comparaciones de muestras genuinas e impostoras respectivamente.

El funcionamiento de la aplicación desarrollada es el siguiente. Los ficheros que contienen los valores de similitud resultados de haber realizado las diferentes comparaciones (ficheros

de formato .txt) son leídos por este programa y se almacenan dichos valores en dos matrices, una para el fichero de genuinos y otra para el de impostores. A partir de estas matrices y mediante el empleo de una serie de funciones, son calculadas las tasas de rendimiento y representadas en gráficas que se muestran al usuario por pantalla, cumpliendo así los requisitos especificados en el apartado 3. Concretamente se representan las gráficas de las curvas FAR vs FRR, ROC y DET, ya que para este trabajo sólo son necesarias las tasas de error relativas a la verificación. En estas gráficas se muestran los resultados obtenidos de las dos rutas introducidas, permitiendo al usuario realizar comparaciones. Además, se muestra en cada una de las imágenes una leyenda que indica qué valor representa cada curva de la gráfica. En caso de las gráficas FAR vs FRR, se ha decidido generar una gráfica para cada experimento debido a que en una misma gráfica es difícil poder comparar los resultados debido a la similitud de los mismos.

Para este trabajo no ha sido necesario obtener los tiempos de rendimiento, ya que al trabajar a partir de imágenes de una base de datos, los tiempos en procesar las huellas son similares en los diferentes casos.

Para poder estudiar la influencia de los dispositivos habría que haber medido el tiempo que tarda cada sensor en capturar la muestra.

Como ejemplo de las gráficas que se obtienen se muestran las siguientes ilustraciones.

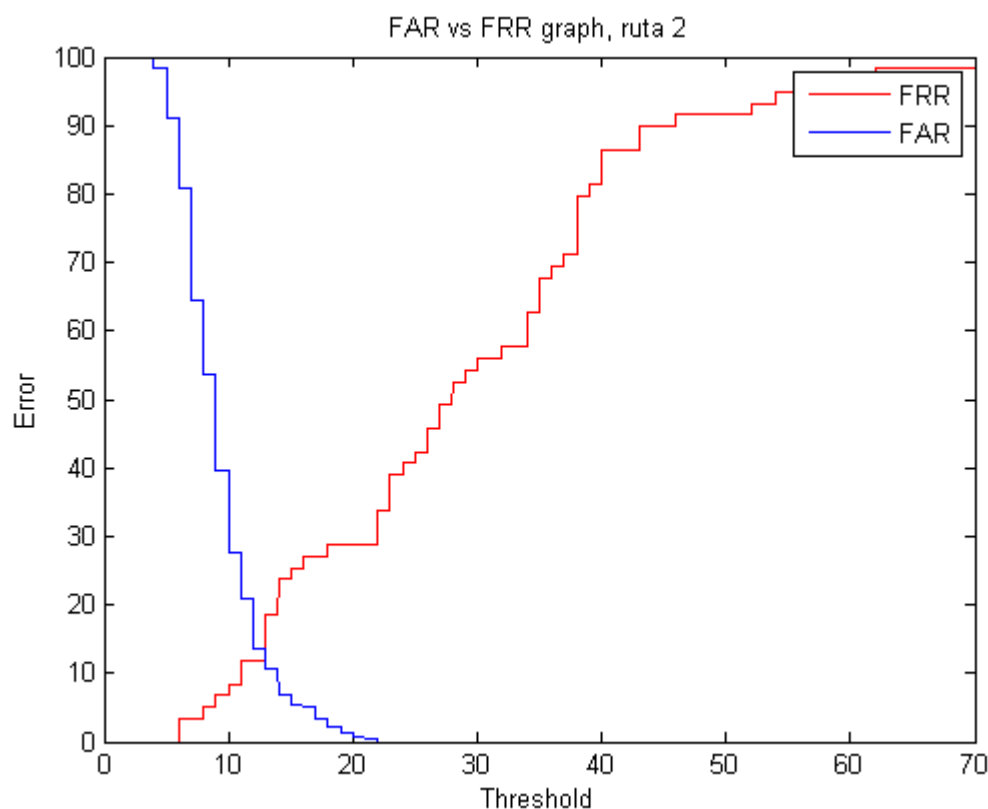


Ilustración 31. Ejemplo gráfica FAR vs FRR

Esta gráfica permite obtener un punto de equilibrio para el rendimiento del sistema. Como se explicó en el apartado 2, la FRR representa las transacciones genuinas incorrectamente denegadas mientras que la FAR representa las transacciones de impostor incorrectamente aceptadas. Por tanto, el punto de corte entre ambas curvas es el punto en el que el sistema tiene un mejor rendimiento (menor tasa de error de falsa aceptación y de falso rechazo). Este punto es denominado como EER. En caso de que el umbral sea más bajo, la tasa de falso rechazo disminuye mientras que la tasa de falsa aceptación aumenta. Es decir se favorece la usabilidad del sistema. Por otro lado, en caso de que el umbral sea más alto aumenta la tasa de falso rechazo, pero la tasa de falsa aceptación disminuye, es decir que se perjudica la usabilidad y se favorece la seguridad.

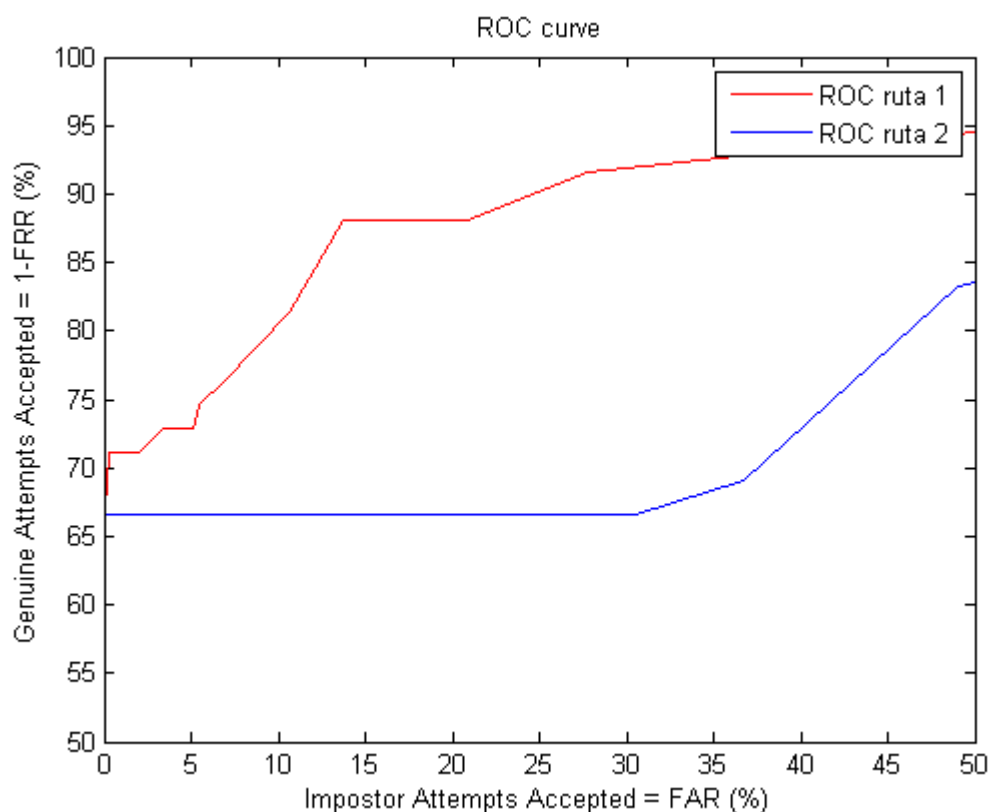


Ilustración 32. Ejemplo curva ROC

La curva ROC compara el porcentaje de comparaciones genuinas que se aceptan correctamente con el porcentaje de comparaciones de impostor que se aceptan incorrectamente. La curva ideal debería comenzar en un valor de 1-FRR del 100%, por lo que el rendimiento será mejor para una curva cuyos valores más se acerquen al 100% en el eje y (eje de ordenadas).

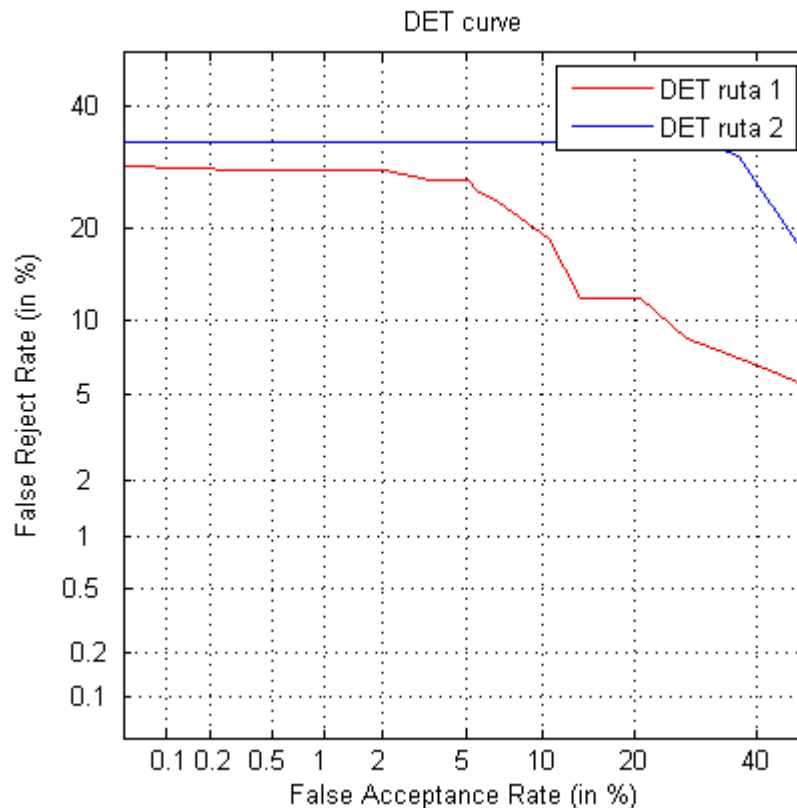


Ilustración 33. Ejemplo curva DET

La curva DET es similar a la curva ROC, con la diferencia de que se compara el porcentaje de comparaciones rechazadas incorrectamente y el porcentaje de comparaciones aceptadas incorrectamente. Además, la curva DET suele presentar una mayor linealidad que la curva ROC, por lo que ayuda a visualizar mejor los resultados en el caso de que las curvas estén muy juntas. Teniendo en cuenta estas diferencias, la curva DET ideal sería la más cercana al 0% en ambos ejes. Cuanto más cerca esté de este valor mejor será el rendimiento.

También hay que mencionar que esta curva permite obtener el EER. Esto se consigue trazando una función $X=Y$. El punto donde se corten dicha función y la curva DET será el EER. Esta técnica es necesaria en caso de que la curva FAR vs FRR no permita saber el EER fácilmente.

5 Pruebas

En este apartado se van a explicar los resultados de las pruebas que se han llevado a cabo para conseguir el objetivo de este trabajo, es decir, el cálculo de la interoperabilidad de los sistemas biométricos basados en huella dactilar. Dichas pruebas, como se ha explicado anteriormente, permiten comparar las tasas de rendimiento obtenidas en distintos experimentos. En este caso, se han llevado a cabo 2 pruebas distintas, para poder comprobar el rendimiento de los sistemas biométricos de huella planar y rodada, tanto si el reclutamiento ha sido llevado a cabo con un mismo sensor, o con un sensor distinto.

Es decir, la primera prueba consiste en comparar las tasas de rendimiento obtenidas cuando el reclutamiento y la verificación se han realizado con el mismo dispositivo. Esta prueba se realiza con dos experimentos. En uno de ellos se llevan a cabo el reclutamiento y la verificación con huellas planares mientras que en el otro experimento se realizan con huellas rodadas.

La segunda prueba permite comparar las tasas cuando el reclutamiento se ha producido con un sensor y la verificación con otro distinto. Al igual que la prueba 1, esta prueba consiste en dos experimentos. En uno de ellos el reclutamiento se lleva a cabo con huellas planares y la verificación con huellas rodadas. En el otro experimento se realiza el reclutamiento con huellas rodadas y la verificación con huellas planares.

Se tendrá en cuenta la base de datos completa y las 3 visitas de verificación para conseguir que los resultados sean más significativos.

También es necesario mencionar que se utilizará el formato NIST para obtener mejores resultados.

5.1 Prueba 1

Como se ha dicho anteriormente, la prueba 1 permite comparar los resultados cuando el reclutamiento se lleva a cabo con un dispositivo de huella planar o rodada, produciéndose la verificación con el mismo dispositivo que en el reclutamiento. En la Ilustración 34 se puede ver un esquema de la prueba.

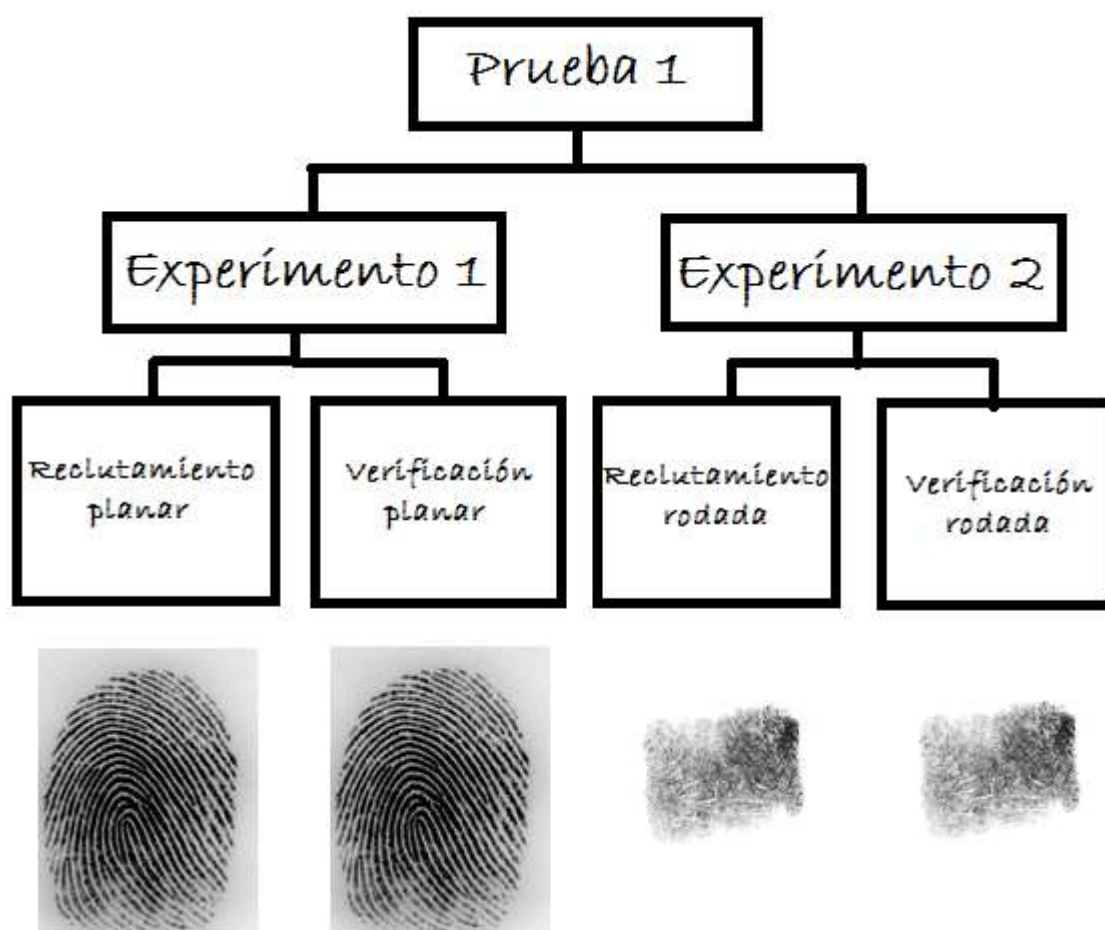


Ilustración 34. Esquema prueba 1

A continuación se pueden observar los resultados obtenidos.

5.1.1 Resultados Experimento 1

En la Ilustración 35 se presenta la curva FAR vs FRR para el experimento 1.

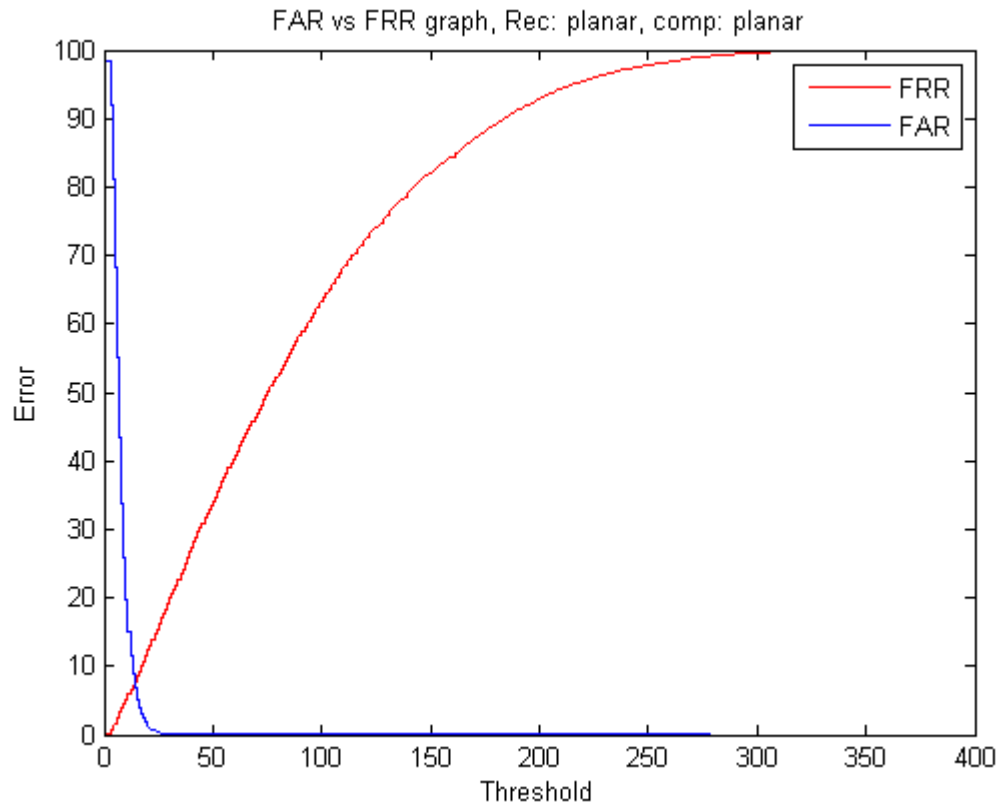


Ilustración 35. Gráfica FAR vs FRR experimento 1 prueba 1

En este experimento, tanto el reclutamiento como la verificación se llevan a cabo con un dispositivo de huella planar.

El EER en este caso es aproximadamente el 8%, ya que en ese punto es en el que se cruzan las curvas FRR y FAR. Este será el punto en el que el sistema tendrá mejor rendimiento.

5.1.2 Resultados Experimento 2

En la Ilustración 36 se presenta la curva FAR vs FRR para el experimento 2.

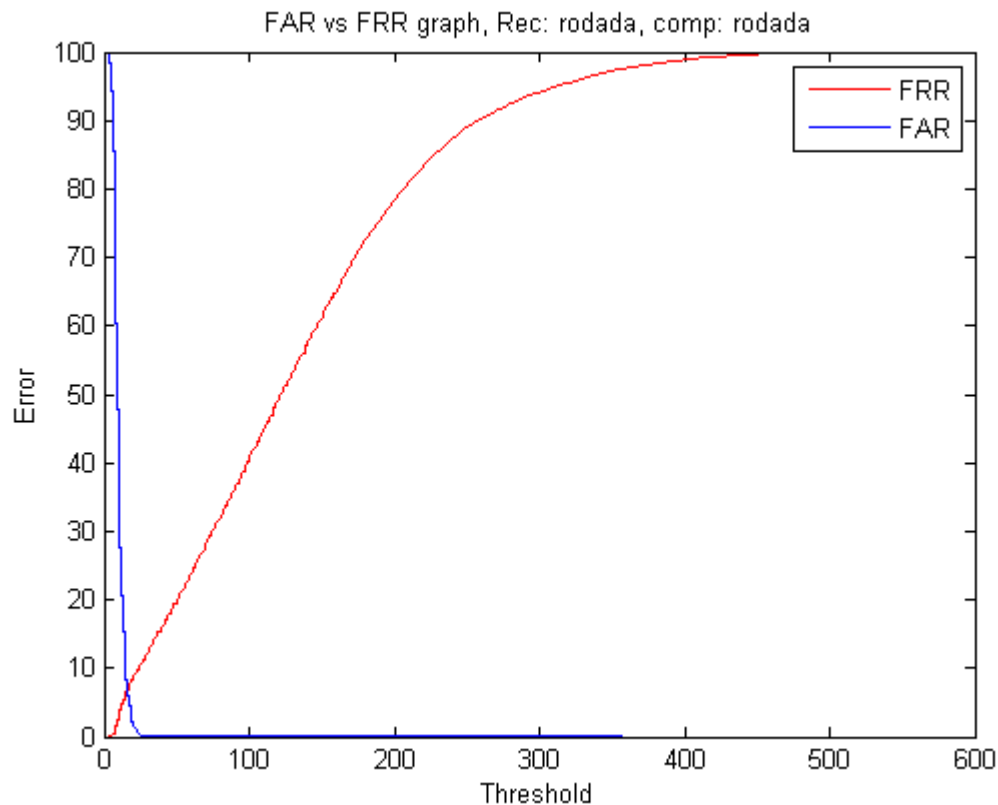


Ilustración 36. Gráfica FAR vs FRR experimento 2 prueba 1

En este experimento, tanto el reclutamiento como la verificación se llevan a cabo con un dispositivo de huella rodada.

El EER es aproximadamente el 7%.

Esta gráfica permite deducir que el rendimiento es algo mejor utilizando huellas rodadas que empleando huellas planares, debido a los valores de EER en los dos experimentos. Esto puede ser debido a que la información de la huella rodada es mayor ya que el sensor toma una mayor superficie del dedo.

5.1.3 Resultados Prueba 1

En la Ilustración 37 se presenta la curva ROC para la prueba 1.

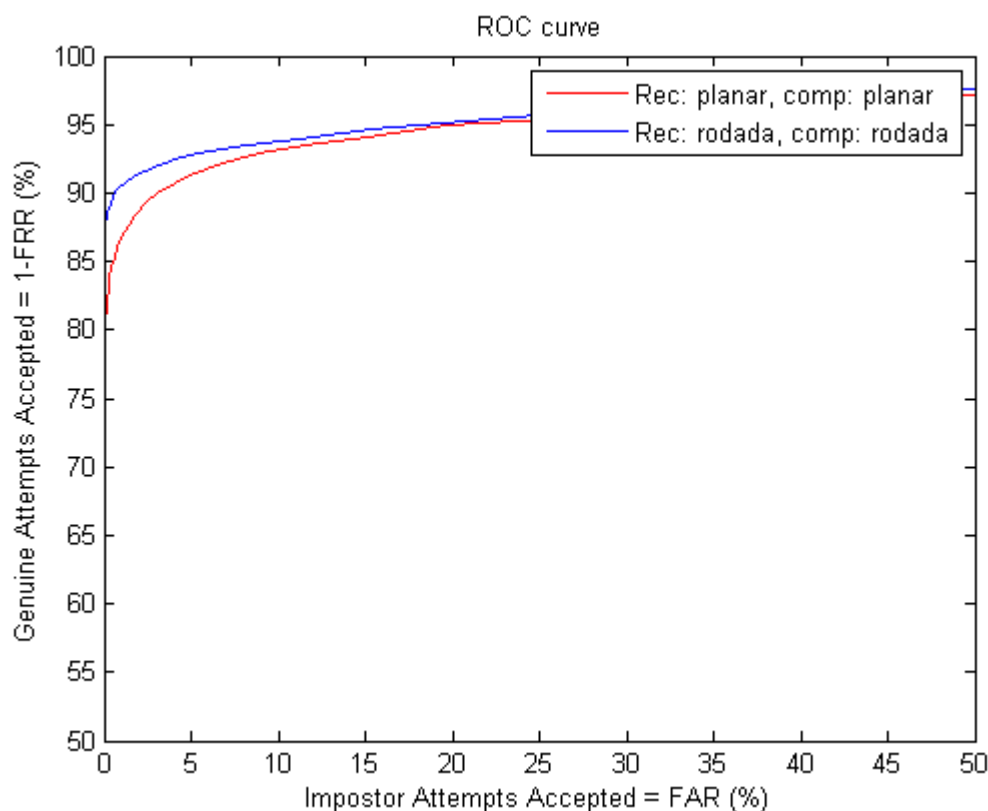


Ilustración 37. Curva ROC prueba 1

En esta gráfica se representa la curva ROC cuando el reclutamiento y la verificación se ha realizado con huellas planares (curva roja) y la curva ROC cuando se han utilizado huellas rodadas (curva azul).

En ninguno de los dos casos se alcanza la curva ideal, ya que en el caso de huellas planares el valor de 1-FRR, cuando la FAR tiene un valor de 0%, es del 81% aproximadamente y en el caso de huellas rodadas el valor ronda el 88%.

La gráfica representa los dos experimentos en conjunto. Como ya se había visto anteriormente, el experimento 2 (curva de color azul) tiene mejores resultados de rendimiento ya que su curva se acerca más a la ideal.

En la Ilustración 38 se presenta la curva DET para la prueba 1.

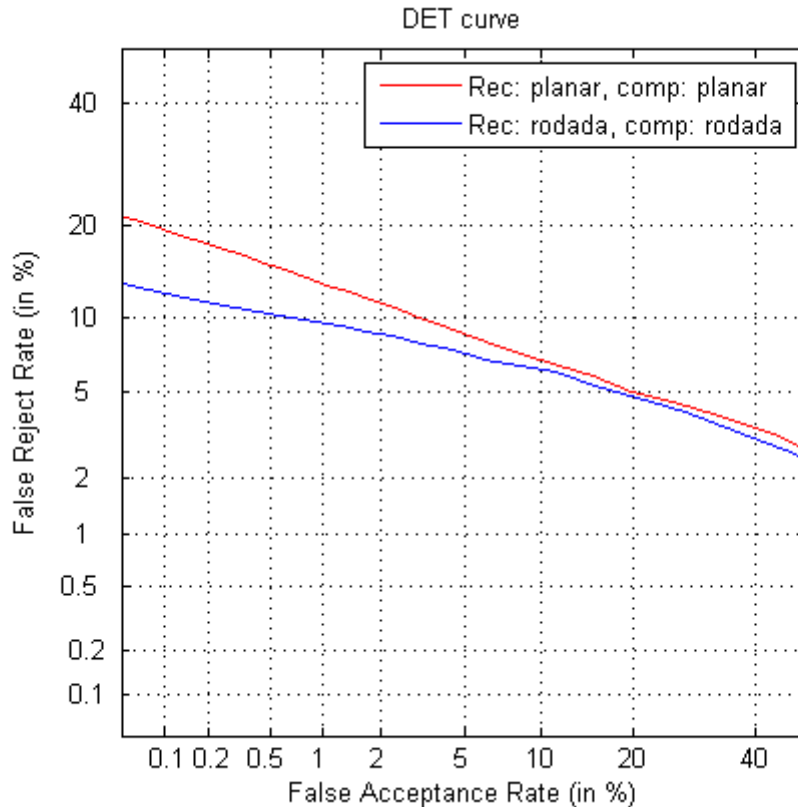


Ilustración 38. Curva DET prueba 1

En esta gráfica se representa la curva DET cuando el reclutamiento y la verificación se ha realizado con huellas planares (curva roja) y la curva DET cuando se han utilizado huellas rodadas (curva azul).

Ninguna de estas curvas se acerca a la curva DET ideal ya que los valores aproximados de la tasa de falso rechazo, cuando el valor de la tasa de falsa aceptación es del 0%, son del 21% para huellas planares y del 14% para huellas rodadas, alejándose ambas del origen.

No obstante, el mejor rendimiento es para la curva del experimento 2. Es decir, que para el caso de reclutar con rodada y verificar con rodada, los resultados son mejores.

Asimismo, en esta curva podemos comparar el EER de ambos experimentos, comprobando lo que ya se había mencionado en el análisis de cada prueba.

En el caso de huellas planares el EER es del 8%, mientras que para huellas rodadas es del 7%, tal como se pudo comprobar en la gráfica FAR vs FRR.

5.1.4 Conclusiones Prueba 1

Como conclusión a esta prueba hay que tener en cuenta que al usar huellas rodadas el número de errores es más bajo, ya que las huellas poseen mayor información que las planares y es más difícil que se realicen comparaciones erróneas.

5.2 Prueba 2

La prueba 2 permite comparar las diferencias cuando el reclutamiento se lleva a cabo con un dispositivo de huella planar o rodada, produciéndose la verificación con un dispositivo de huellas de distinto tipo que las de la verificación. En la Ilustración 39 se puede ver un esquema de la prueba.

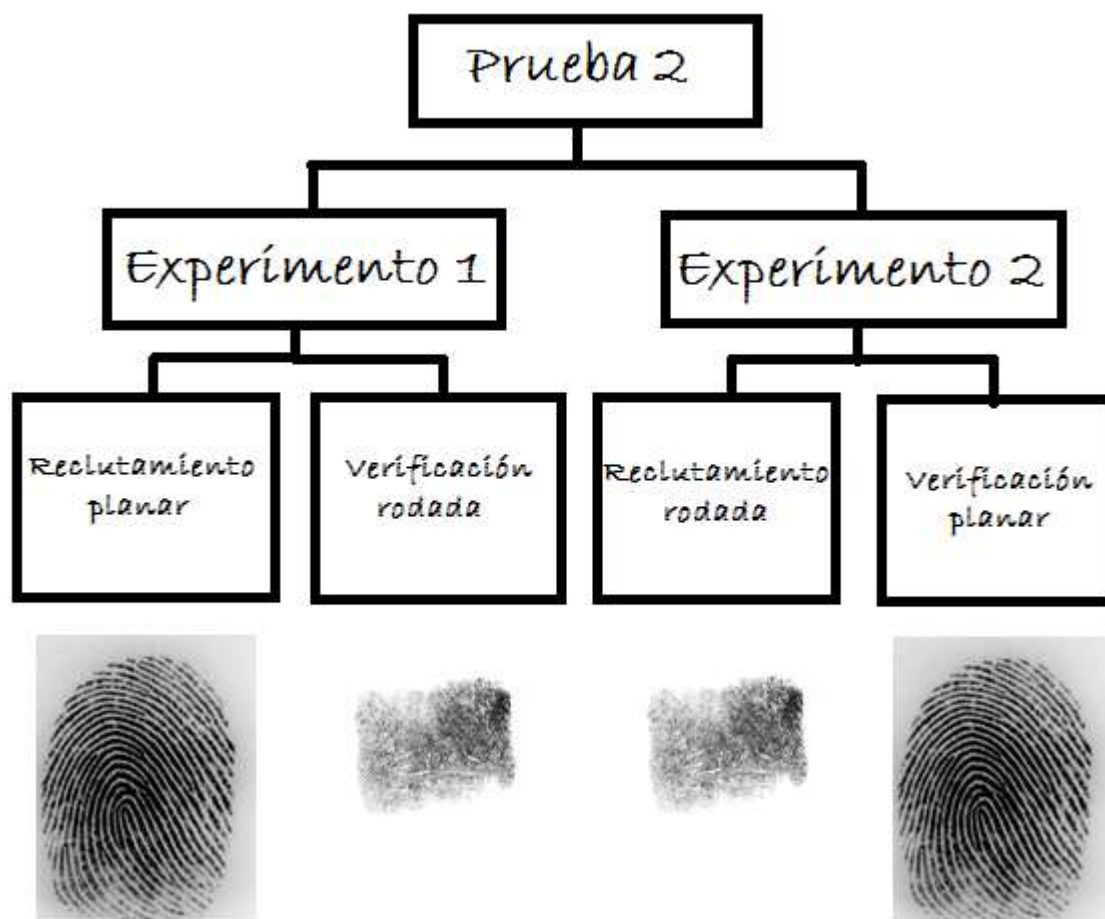


Ilustración 39. Esquema prueba 2

A continuación se pueden observar los resultados obtenidos.

5.2.1 Resultados Experimento 1

En la Ilustración 40 se presenta la curva FAR vs FRR para el experimento 1.

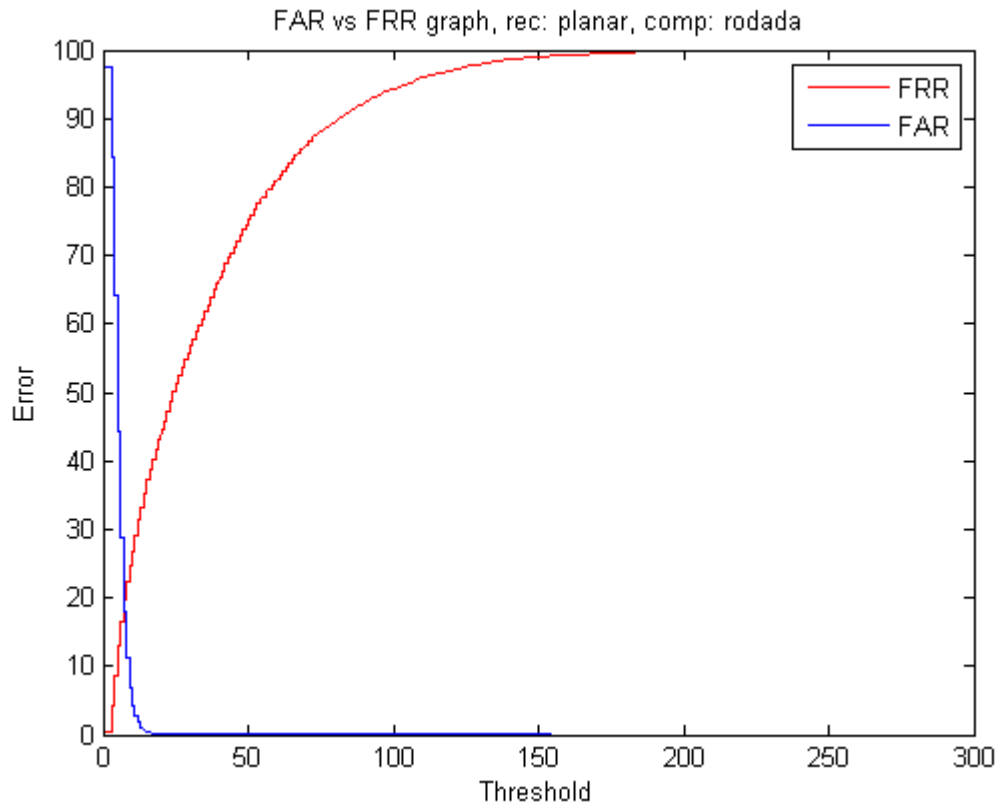


Ilustración 40. Gráfica FAR vs FRR experimento 1 prueba 2

En este experimento, el reclutamiento se lleva a cabo con huellas planares y la verificación con huellas rodadas.

En este caso, se puede observar que los resultados son muy parecidos a los de la prueba 1, pero que el número de transacciones incorrectamente denegadas, representado por la FRR, es algo mayor que en la prueba anterior. Por su parte, las transacciones de impostor incorrectamente aceptadas también son algo mayores en este caso.

El valor del EER para este caso será del 19% aproximadamente, siendo bastante más elevado que en cualquiera de los dos experimentos de la Prueba 1.

5.2.2 Resultados Experimento 2

En la Ilustración 41 se presenta la curva FAR vs FRR para el experimento 2.

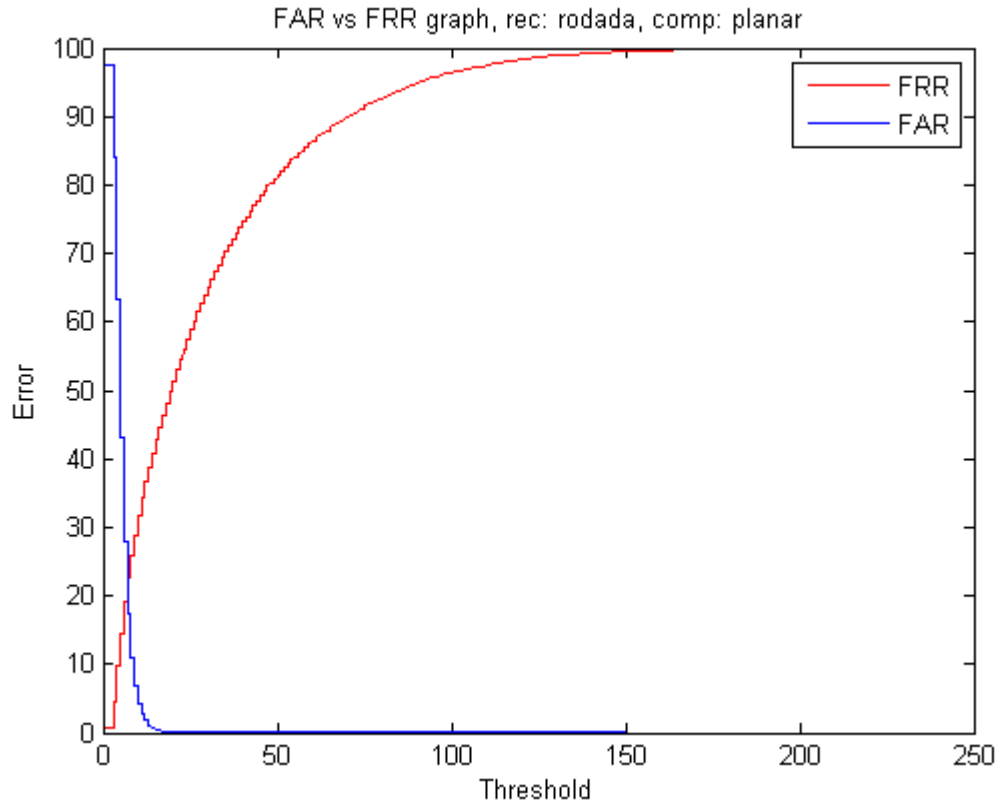


Ilustración 41. Gráfica FAR vs FRR experimento 2 prueba 2

En este experimento, el reclutamiento se lleva a cabo con huellas rodadas y la verificación con huellas planares.

En este experimento ocurre lo mismo que en el anterior, los errores son más altos que cuando se realizan el reclutamiento y la verificación con el mismo sensor. Además los errores son más altos cuando se produce el reclutamiento con huellas rodadas y la verificación con huellas planares que en el caso contrario.

El valor del EER es del 22% aproximadamente, por lo que el rendimiento es peor en este caso que en el Experimento 1.

5.2.3 Resultados Prueba 2

En la Ilustración 42 se presenta la curva ROC para la prueba 2.

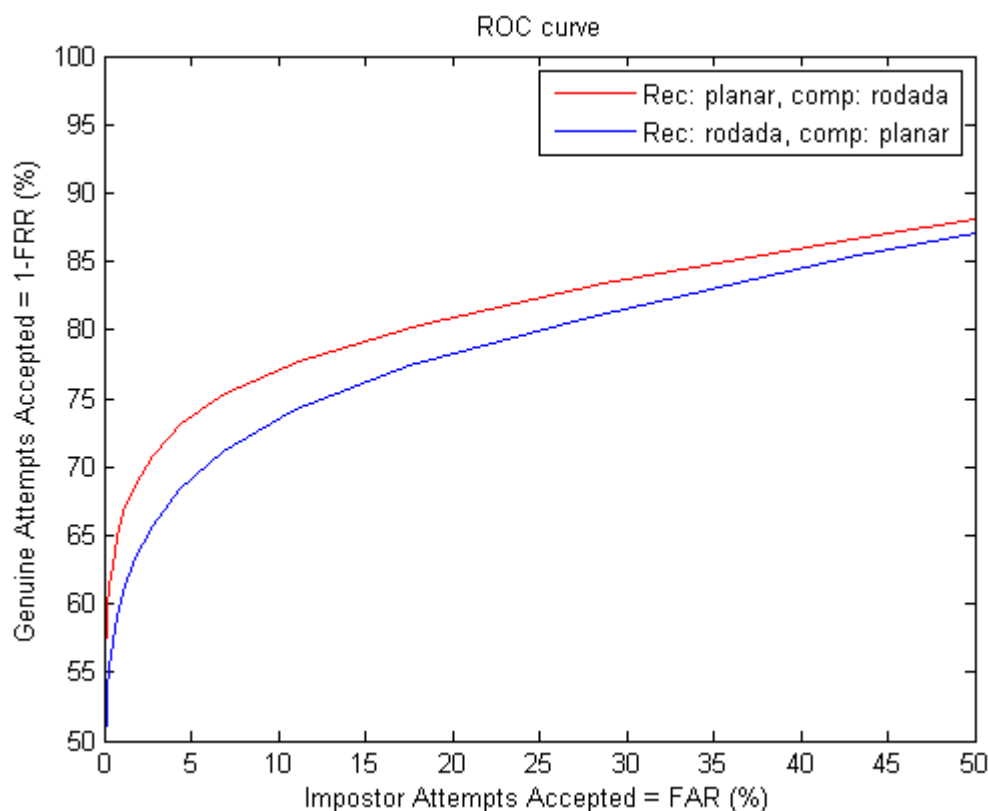


Ilustración 42. Curva ROC prueba 2

En esta gráfica se representa la curva ROC cuando el reclutamiento se realiza con huellas planares y la verificación con huellas rodadas (curva roja) y la curva ROC cuando el reclutamiento se realiza con huellas rodadas y la verificación con huellas planares (curva azul).

En ninguno de los dos casos se alcanza la curva ideal, ya que cuando se realiza el reclutamiento con planar y la verificación con rodada el valor de 1-FRR, cuando la FAR tiene un valor de 0%, es del 57,5% aproximadamente mientras que en el caso contrario es del 51%.

La gráfica representa los dos experimentos en conjunto. Como ya se había visto anteriormente, el experimento 1 (curva de color rojo) tiene mejores resultados de rendimiento ya que su curva se acerca más a la ideal.

En la Ilustración 43 se presenta la curva DET para la prueba 2.

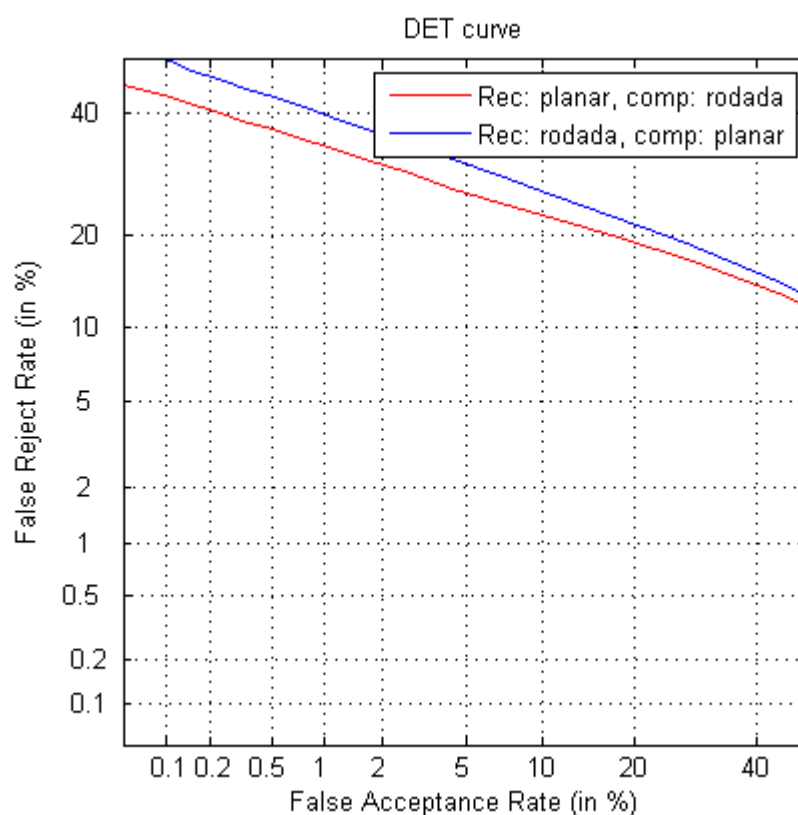


Ilustración 43. Curva DET prueba 2

En esta gráfica se representa la curva DET cuando el reclutamiento se realiza con huellas planares y la verificación con huellas rodadas (curva roja) y la curva ROC cuando el reclutamiento se realiza con huellas rodadas y la verificación con huellas planares (curva azul).

Ninguna de estas curvas se acerca a la curva DET ideal ya que los valores de la tasa de falso rechazo, cuando el valor de la tasa de falsa aceptación es del 0%, son superiores al 40%, alejándose ambas del origen.

No obstante, el mejor rendimiento es para la curva del experimento 1. Es decir, que para el caso de reclutar con planar y verificar con rodada, los resultados son mejores.

Asimismo, en esta curva podemos comparar el EER de ambos experimentos, comprobando lo que ya se había mencionado en el análisis de cada prueba.

El EER cuando el reclutamiento se realiza con huellas planares y la comparación con huellas rodadas es del 19% mientras que en el caso contrario es del 22% aproximadamente, tal como se mencionó en la gráfica FAR vs FRR.

5.2.4 Conclusiones Prueba 2

Por tanto, como conclusión para la prueba 2 hay que resaltar dos ideas. La primera de ellas es que el rendimiento al realizar reclutamiento y verificación con sensores distintos es mucho menor que cuando se emplea el mismo tipo de sensor, ya que se producen mayor cantidad de errores.

Por otro lado, el rendimiento al llevar a cabo el reclutamiento con huellas planares y la verificación con huellas rodadas es mayor que en el caso contrario. Esto puede ser debido a que las huellas rodadas contengan más información que las planares, por lo que al realizar la verificación con huella planar podría faltar información para poder aceptar la comparación.

5.3 Comparación Prueba 1 con Prueba 2

A continuación se muestra una tabla con un resumen de los resultados obtenidos.

Tabla 3. Resumen de los resultados

	Prueba 1		Prueba 2	
	Exp. 1	Exp. 2	Exp. 1	Exp. 2
Reclutamiento	Planar	Rodada	Planar	Rodada
Verificación	Planar	Rodada	Rodada	Planar
EER	8%	7%	19%	22%

Los resultados anteriores muestran que es bastante mejor el rendimiento cuando se usa el mismo tipo de sensor para el reclutamiento y la verificación que cuando se usan distintos sensores.

Los mejores resultados se han obtenido para los siguientes experimentos:

- Reclutamiento con rodada y verificación con rodada en caso de usar el mismo sensor.
- Reclutamiento con planar y verificación con rodada en caso de usar distintos sensores.

Si se utilizan los mismos sensores lo mejor es utilizar la huella rodada porque aporta más información que la huella planar, siendo más difícil que se produzcan errores.

Si se utilizan sensores distintos lo mejor es llevar a cabo el reclutamiento en planar y la verificación con rodada. Esto se debe en primer lugar a que la interacción del usuario con el sensor de captura es más fácil cuando simplemente tiene que posar la huella frente a tener que rodarla. Como resultado se obtiene un patrón de mejor calidad. Por otro lado, la información para el proceso de comparación es más completa en el caso de la huella rodada. Por lo que

aunque la huella resulte de peor calidad, es posible obtener un mayor número de minucias y reducir el error a la hora de compararla con el patrón.

Sin embargo, para obtener unos resultados generales habría que realizar el estudio con otro tipo de dispositivos para confirmar si esta conclusión se mantiene.

6 Conclusiones y líneas futuras

6.1 Conclusiones

Tras realizar este trabajo se han podido obtener algunas conclusiones.

Se ha podido estudiar la interoperabilidad de sensores de huella planar y rodada atendiendo a las diferentes normativas que eran necesarias para este TFG. Para ello, a partir de una base de datos que contiene huellas de diferentes usuarios, tomadas con diferentes sensores y de formas distintas (huella planar y rodada), se ha desarrollado una aplicación que obtuviera los valores de similitud resultantes al comparar unas huellas con otras. Posteriormente, se ha desarrollado una aplicación que obtiene las tasas de rendimiento necesarias para este trabajo. Por último, se han llevado a cabo una serie de pruebas para analizar los resultados de las tasas de rendimiento para distintos casos, permitiendo analizar el rendimiento cuando el reclutamiento y la verificación se realizan con el mismo tipo de dispositivo y cuando se llevan a cabo con distinto tipo de dispositivo. Estos pasos han permitido cumplir con todos los requisitos que eran necesarios para la realización de este trabajo.

En relación con los resultados obtenidos, las gráficas finales muestran como el rendimiento es mayor al realizar el reclutamiento y la verificación con el mismo sensor ya que tiene las mismas características y, por tanto, el número de errores al comparar las huellas es mucho menor.

Por otro lado, también hay que tener en cuenta que el sensor de huellas rodadas tiene mejor rendimiento que el de huellas planares ya que se obtiene mayor superficie de huella en sus muestras y por tanto el error es menos común.

Sin embargo, el sensor de huellas rodadas es mucho más difícil de usar para los usuarios y provoca por ello más errores en el reclutamiento de muestras, por lo que el número de muestras obtenidas es menor. Además, el proceso de reclutamiento y verificación es más largo y la mayor parte de los usuarios no tienen una buena experiencia con este sensor.

6.2 Líneas futuras

Algunas líneas futuras de investigación que podrían llevarse a cabo están relacionadas con la realización de más pruebas para mejorar los diferentes sistemas de identificación biométrica.

Por un lado, se debería realizar un estudio del rendimiento de otros dispositivos de huella dactilar, tanto si son de la misma tecnología que los utilizados para comprobar si las conclusiones obtenidas se mantienen, como para otros dispositivos de distinta tecnología como son los capacitivos.

Además, también podría llevarse a cabo un estudio empleando otros tipos de sistema de identificación, como el de iris o geometría de la mano.



También, para conseguir una mayor fiabilidad, se debería realizar un estudio con una base de datos con mayor número de usuarios que puedan poseer características distintas, como el color de la piel, enfermedades, etc.

Por último, en función a los resultados obtenidos, se debería intentar mejorar el funcionamiento de los sistemas biométricos para que el rendimiento sea más alto.

Bibliografía

- [1] Actualidades de la UIT. <http://www.itu.int/net/itunews/issues/2010/01/05-es.aspx>, Consultado: 7 de octubre de 2013
- [2] ISO, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50873, Consultado: 28 de enero de 2014
- [3] Cuida tus datos. <http://www.cuidatusdatos.com/lopdl/>, Consultado: 7 de octubre de 2013
- [4] María José, Seguridad en la red para principiantes, <http://security-for-dummies.blogspot.com.es/> , última consulta: 27 de octubre de 2013
- [5] Sistemas biométricos.cl Biometría en el mundo, <http://www.sistemasbiometricos.cl/web/2010/01/18/lector-de-adn-en-30-minutos/>, última consulta: 17 de noviembre de 2013
- [6] Esolva.com, <http://www.esolva.com/firmas/>, última consulta: 17 de noviembre de 2013
- [7] Biometria - Reconocimiento de Íris, http://www.gta.ufrj.br/grad/08_1/iris/, última consulta: 17 de noviembre de 2013
- [8] Olx, <http://coyoacan.olx.com.mx/cheCADOR-de-asistencia-biometrico-de-huella-digital-iid-150994902>, última consulta: 17 de noviembre de 2013
- [9] Sánchez Reíllo, Raúl, Identificación Biométrica
- [10] Fernández Saavedra, M^a Belén, Evaluación de los Sistemas de Identificación Biométrica
- [11] Fernández Saavedra, M^a Belén, Biometría y la evaluación de los sistemas biométricos
- [12] BiometricSupply, BiometricSupply, <http://www.biometricsupply.com/suprema-biomini-plus.html>, última consulta:30 de octubre de 2013
- [13] Serteck tecnología, Serteck tecnología,<http://www.serteck.com.mx/v3/component/virtuemart/biometria/huella-y-proximidad/hamster-4-detail?Itemid=0>, última consulta:30 de octubre de 2013
- [14] Terabyte, Terabyte Soluciones en Tecnologías de la Información, <http://www.solucionesterabyte.com/biometricos.html>, última consulta:30 de octubre de 2013
- [15] Choozen, <http://www.choozen.es/ts-lector-huella-digital~informatica,2000000.html>, última consulta: 30 de octubre de 2013
- [16] Wikipedia - Microsoft Visual Studio. http://es.wikipedia.org/wiki/Microsoft_Visual_Studio , Consultado: 10 de octubre de 2013



-
- [17] Wikipedia - Matlab, <http://es.wikipedia.org/wiki/MATLAB> , Consultado: 10 de octubre de 2013
 - [18] Sourceforge, <http://ffpis.sourceforge.net/man/mindtct.html>, Consultado: 29 de enero de 2014
 - [19] NIST, <http://www.nist.gov/itl/iad/ig/nbis.cfm>, Consultado: 29 de enero de 2014
 - [20] La web de Maco048, <http://www.marisolcollazos.es/articulos/Investigacion-criminologica/Nuevo-estandar-datos-biometricos.html>, Consultado: 17 de enero de 2014

Anexo A: Planificación

A continuación se detallará el tiempo aproximado empleado en cada tarea de este trabajo.

Fase 1: Documentación inicial

- I. Asistencia a charlas y presentaciones sobre Biometría (10 horas)
- II. Estudio de la Biometría (10 horas)
- III. Preparación de las herramientas de trabajo (3 horas)

Fase 2: Obtención de la base de datos

- I. Explicación y aprendizaje de la aplicación de recogida de huella (2 horas)
- II. Recogida de huellas (50 horas)

Fase 3: Desarrollo de las aplicaciones

- I. Obtención de minucias y valores de comparación (30 horas)
- II. Obtención de tasas de rendimiento (20 horas)
- III. Pruebas de las aplicaciones (5 horas)
- IV. Mejora de las aplicaciones (30 horas)

Fase 4: Pruebas finales

- I. Obtención de resultados de comparación de los experimentos (20 horas)
- II. Estudio de los resultados (20 horas)

Fase 5: Elaboración de la memoria

- I. Redacción de la memoria (80 horas)
- II. Corrección (20 horas)

Tabla 4. Duración del proyecto

FASES	HORAS EMPLEADAS
Documentación inicial	23
Obtención de la base de datos	52
Desarrollo de las aplicaciones	85
Pruebas finales	40
Elaboración de la memoria	100
TOTAL	300

Anexo B: Presupuesto

Costes materiales

Para este trabajo ha sido necesario el uso 3 ordenadores y 4 dispositivos de huella dactilar. Debido a que el tiempo de amortización de cada uno de los ordenadores y dispositivos será de 4 años, los resultados serán los obtenidos en la Tabla 5.

Tabla 5. Costes materiales

CONCEPTO	PRECIO (€)
2 ordenadores de altas prestaciones	200
Ordenador de bajas prestaciones	50
4 dispositivos de huella dactilar	200
TOTAL	450

Costes de personal

Para realizar este trabajo ha sido necesario el trabajo de un ingeniero y de un jefe de proyecto.

Tabla 4. Costes de personal

OCUPACIÓN	HORAS	PRECIO/HORA	PRECIO (€)
Ingeniero	280	50	14.000
Jefe de proyecto	20	90	1.800
TOTAL	300		15.800

Costes totales

Tabla 5. Costes totales

Concepto	PRECIO (€)
Costes materiales	450
Costes de personal	15.800
Costes indirectos (20%)	3.250
Subtotal	19.500
IVA (21%)	4095
TOTAL	23.595